CA92276-8604-02

PRIMERGY

スイッチブレード (1Gbps 36/8+2) (PG-SW111)
スイッチブレード (1Gbps 36/12) (PG-SW112)

IBP ユーザーズガイド

FUJITSU

本書をお読みになる前に

外国為替及び外国貿易法に基づく特定技術について

当社のドキュメントには「外国為替および外国貿易管理法」に基づく特定技術が含まれていることがあります。特定技術が含まれている場合は、当該ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

本書の内容について

このたびは、弊社の PRIMERGY スイッチブレード (1Gbps 36/8+2) ／PRIMERGY スイッチブレード (1Gbps 36/12) をお買い上げいただき、誠にありがとうございます。
本書は、本製品が IBP モードに設定されている場合のコマンド使用方法を示した、IBP ユーザーズガイドのマニュアルです。なお、本文は英語で記載しています。
本書をよくお読みになり、正しい取り扱いをされますようお願いいたします。

■ 関連マニュアル

- PRIMERGY スイッチブレード (1Gbps 36/8+2) (PG-SW111)／PRIMERGY スイッチブレード (1Gbps 36/12) (PG-SW112) 取扱説明書
- PRIMERGY スイッチブレード (1Gbps 36/8+2) (PG-SW111)／PRIMERGY スイッチブレード (1Gbps 36/12) (PG-SW112) スイッチユーザーズガイド
- PRIMERGY スイッチブレード (1Gbps 36/8+2) (PG-SW111)／PRIMERGY スイッチブレード (1Gbps 36/12) (PG-SW112) スイッチコンフィグレーションガイド
- PRIMERGY スイッチブレード (1Gbps 36/8+2) (PG-SW111)／PRIMERGY スイッチブレード (1Gbps 36/12) (PG-SW112) IBP コンフィグレーションガイド

上記マニュアルは「PRIMERGY」ページの「マニュアル」(http://primeserver.fujitsu.com/primergy/manual.html) からご覧ください。

PRIMERGY ブレード･サーバ･システム

IBPユーザーズガイド

2010年12月版

著作権・商標

著作権© 2010 Fujitsu Technology Solutions GmbH.

デリバリは可用性により異なります。技術的変更を実施する権利が保持されます。

© 2010 富士通テクノロジー・ソリューションズ

目次

© 2010 富士通テクノロジー・ソリューションズ

© 2010 富士通テクノロジー･ソリューションズ

1　　重要な注意事項

この取説は装置の近くに保管すること。 第三者に装置を渡す場合、この取説もともに渡すこと。 この頁を注意してよく読み、装置を開梱する前に情報のﾒﾓを取ること。 まず装置を開いてからでないとｽｲｯﾁ･ﾌﾞﾚｰﾄﾞにはアクセスできない。 この取扱説明書の「重要な注意事項」の章にある安全中事項に従うこと。 部品は稼動中に極めて高温になる。 装置を取り扱う際は部品に触らないこと。 火傷の危険がある。 設置中に装置が損傷した場合保証は無効となる。

1.1　　ボードについて

装置または部品と部品に実装されている導電部品を損傷しないために、これらを挿入または取外すときは注意深く行うこと。 ボードが真っ直ぐｽﾛｯﾄに装着され、部品または部品にある導電部品、または他の部品を損傷しないことに十分注意すること。 ボードを交換するときはロック機構 (キャッチ、センタリング･ピン等)を丁寧に取り扱うこと。

装置を浮かすときに鋭利な物(ドライバー等)を使用してはならない。 静電により損傷しやすいデバイス(ESD)を実装したボードは表記のラベルにより識別できる。 ESDを実装したボードを取り扱うときは、いかなる事情があっても必ず次の項目に従うこと：

- 作業前には必ず静電気を取り除く(たとえば、接地された物に触る等)こと。
- 設備や工具には静電蓄積が無いこと。
- ESDを実装したボードを挿入したり取外す前に主電源から電源プラグを抜くこと。
- ESD付きボードは常にボードの縁を持つこと。
- ESDを装備したボードにあるピンや導電部品には触らないこと。

1.2　　準拠性宣言

FCC Class A準拠性

この装置はFCC（連邦通信委員会）規則パート15による「クラスA」デジタル装置に課される限界値に準拠することが試験により実証済みであり、(カナダ干渉発生機器規格のすべての要件に合致している。 当該限界値は住宅での接地の際有害な干渉から適格な保護を提供するために設計されている。 この設備は無線周波エネルギーを発生し、使用し、放射し、厳密に指示通りに設置され使用されない場合、無線通信に有害な干渉を発生することがある。 しかし、特定の設置形態では干渉が発生しないという保証は無い。 この設備がラジオやテレビの受信に有害な干渉を発生しうる場合、- これはラジオやテレビの電源を入れたり切ったりするとわかる ー、次のうち一つまたはそれ以上の措置を講じて干渉を是正すること。

– 受信アンテナの方向を変えるまたは場所を移す。
– この設備と受信機をさらに離す。
– この設備を受信機が接続されているのとは別の回路のコンセントに接続する。
– 補助が必要な場合受信機の販売店かラジオやテレビの経験豊かな技術者に相談すること。

富士通テクノロジー・ソリューションズは、この設備の未許諾変更または富士通テクノロジー・ソリューションズが指定したものとは異なる接続コードや設備で代替または接続することから発生したラジオやテレビの干渉からは免責される。 当該の未承諾変更、代替または接続に起因する干渉の是正はユーザーの責任である。

RJ-45接続には非シールド・ツイストペア・ケーブル(UTP) ー 10Mbps接続にはカテゴリ3以上、100Mbps接続にはカテゴリ5以上、1000Mbpsにはカテゴリ5または5e ー を使用できる。



この設備を取り扱う際の静電放電を防止するため静電防止用リスト・ベルトを着用するまたは他の適格な措置を取ること。

インダストリ・カナダ規格クラスA

このデジタル装置は、カナダ通信省ICES003の「デジタル装置」干渉発生装置規格に規定されるデジタル装置からの無線ノイズ発生に対するクラスA限界値を超えない。

日本VCCIクラスA

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

電磁波干渉および安全性(EEC)に関するCEマーク準拠性宣言

この情報技術設備は欧州委員会指令89/336/EECによる電磁両立性に関する加盟国法律の適合化および一定の電圧限界値以内で使用される電気機器に関する指令73/23/EECおおびその修正指令93/68/EECの要件に準拠する。 当該指令との準拠性評価には次の規格を使用した：

- 無線周波数干渉の放出：
  - EN 55022:1998 による限界値クラスA
  - EN 61000-3-2/2006 による高調波放出限界値クラスA
  - EN 61000-3-3/1995 による低電圧電源系の電圧変動やムラの制限
- 電磁波耐性：
  - EN 55024:1998 による製品群規格
  - EN 61000-4-2:1995 による静電放電 (接触放電許容値： ±8 kV、空中放電： ±8 kV)
  - EN 61000-4-3:1995 による無線周波数電磁場許容値 (1 kHz AM 80%変調による 80 - 1000MHz： 3 V/m)
  - EN 61000-4-4:2004 による高速過渡/バースト電圧 (AC/DC電源： ±1 kV、データ:/信号ライン： ±0.5 kV)
  - EN 61000-4-5:1995 によるサージ電磁波耐性試験(AC/DC線間: ±1 kV、AC/DCライン対接地: ±2 kV)
  - 無線周波数場により誘導される伝導妨害による電磁波耐性： EN 61000-4-6:1996 による(1 kHz AM 80%変調による 0.15 - 80 MHz: 3 V/m)
  - EN 61000-4-8:1993 による電源周波数電磁場電磁波耐性試験(50Hz周波数で1A/m)
  - EN 61000-4-11:1994 による電圧降下、短時間の中断、および電圧変動に対する耐性試験 (>95% 減少 @10 ms、30% 減少 @500 ms、 >95% 減少 @5000 ms)
- LVD:
  - EN 60950 (A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)



RF-45ポートに電話用ジャックコネクタを差し込まないこと。 これはポートを損傷する場合がある。 ポートは電話線には使用禁止である。

台湾BSMI クラスA

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

オーストラリアAS/NZS 3548 (1995) - クラスA



© 2010 富士通テクノロジー・ソリューションズ

2 序文

PRIMERGY BX900ブレード･サーバはモジュール構成サーバであり、最大18個のサーバ、8個のコネクション･ブレード(基本仕様に6個のコネクション･ブレードが含まれ、別に2個はオプション)、2個の管理モジュール (MMB)を一体化している。 イーサネット接続ブレード･モジュールはPRIMERGY BX900ブレード･サーバにネットワーク機能とIBP機能を提供する。 管理モジュールはPRIMERGY BX900ブレード･サーバの一点制御点である。PRIMERGY BX900ブレード･サーバは、PRIMERGY BX900 GbEコネクション･ブレード36/8+2スタック(PG-SW111)とPRIMERGY BX900 GbEコネクション･ブレード36/12 (PG-SW112)からなる2種類のイーサネット･コネクション･ブレードを内蔵している。

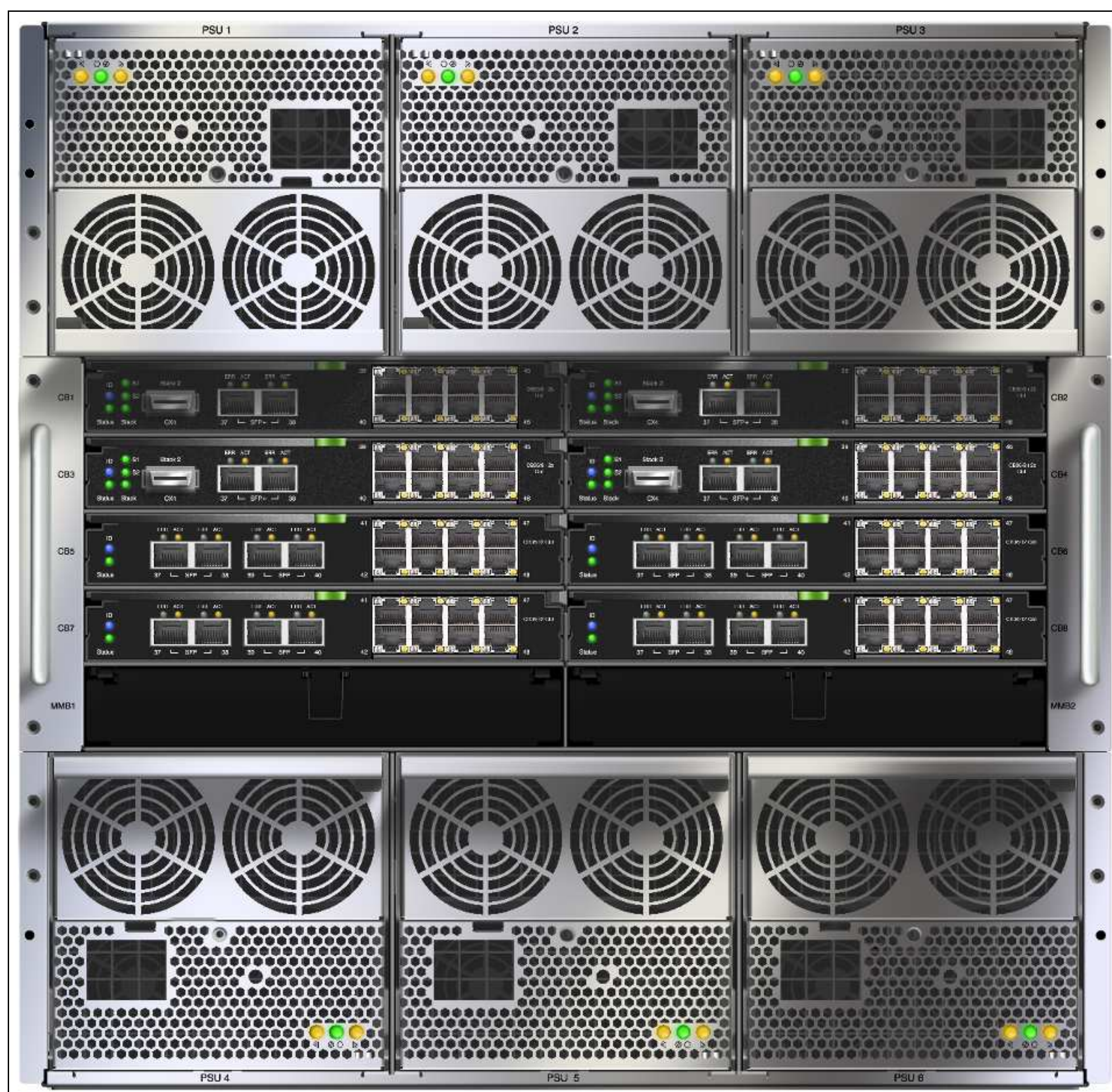


図: BX900 ブレード･サーバの背面

イーサネット･コネクション･ブレードは10Uの次世代型ブレード･サーバのために設計された。 コネクション･ブレードには次に示す2種類ある。

a) PG-SW111 は 46 ポート 1GbE、 2 個の 10GbE SFP+ アップリンク･レイヤー2+スタック可能コネクション･ブレードである。 イーサネット･コネクション･ブレードの構成は中央部に 36 個のダウンリンク･ポート、さらにアップリンク･ポートには RJ45 コネクタによる 8 個の 1GbE および 2 個の 10GbE SFP+からなる。 HiGig/HiGig+ポートが 2 個装備されており、そのうち 1 個は中央部に接続されており、別の 1 個はイーサネット･コネクション･ブレードの背面にありスタック機能を提供する。スタック部は最大 8 個の PG-SW111 スイッチをサポートする。

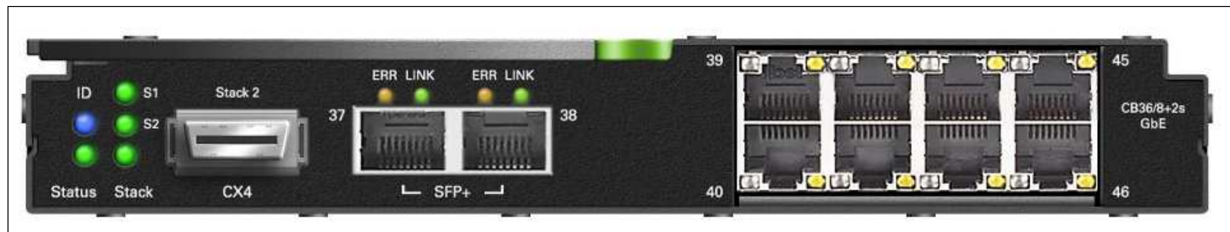


図 ： PRIMERGY BX900 GbEコネクション･ブレードの 36/8+2 スタック(PG-SW111) 前面

b) PG-SW112 は 48 ポート 1GbE、 4 個の 1GbE SFP アップリンク･レイヤー2+イーサネット･コネクション･ブレードである。 イーサネット･コネクション･ブレードの構成は中央部に 36 個のダウンリンク･ポート、さらにアップリンク･ポートには RJ45 コネクタによる 8 個の 1GbE および 4 個の 1GbE SFP からなる。

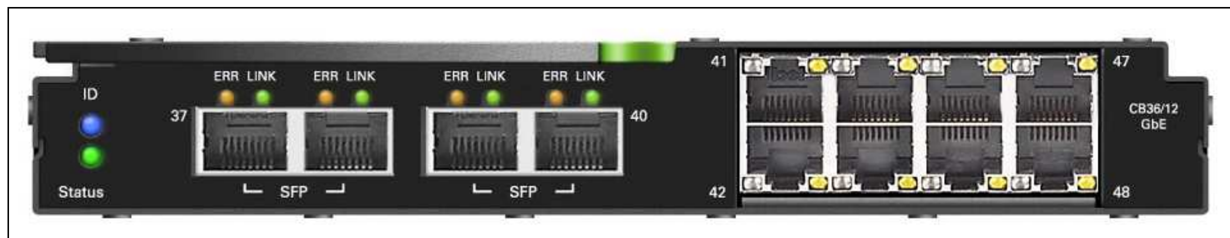


図: PRIMERGY BX900 GbEコネクション･ブレードの 36/12 (PG-SW112) 前面

装置への端末接続はMMBボードのみ可能。 デバッグと管理のために、イーサネット･コネクション･ブレードのUARTバスがMMBボードに接続されている。 MMBボードは同時に1個のみのコネクション･ブレードを管理対象として選択できる。 このイーサネット･コネクション･ブレードはMMB管理用インバンド管理インターフェイスにもなる。

2.1　イーサネット･コネクション･ブレードの機能

このイーサネット･コネクション･ブレードは性能を上げるため多くの高度機能を提供する。 マルチキャスト･フィルタリングはリアルタイムにネットワーク･アプリケーションをサポートします。 ポート･ベースのタグ付きVLAN、さらに自動GVRP VLAN登録サポートによりトラフィックの安全性とネットワーク帯域の効率的使用が可能である。 QoSプライオリティ･キューイングはネットワーク全体でリアルタイムにマルチメディア･データを移動する際の遅延を最小限にできる。 フロー制御によりポートの飽和が引き起こすパケット損失は無い。 さらにブロードキャスト･ストーム抑制によりブロードキャスト･トラフィックがネットワークトラブルを防ぐ管理機能をいくつか紹介します。

Head of Line Blocking

Head of Line Blocking(HOL)は、同一出口ポートのバッファに競合するトラフィックの遅延とフレーム損失を生起させる。 Head of Line Blockingはパケットを順に並べ、キュー先頭パケットはキュー最後のパケットより先に転送される。

フロー制御サポート(IEEE 802.3X)

フロー制御はより高速なデバイスによるパケット送信を抑制して低速デバイスが高速デバイスと通信できるようにする。 伝送はバッファー･オーバーフローを防止するため一時的に停められる。

バックプレッシャ ･サポート

半二重リンクでは、受信ポートは追加的トラフィックにはリンクが利用できないようにリンクを占有してバッファー･オーバーフローを防止する。

ジャンボフレーム･サポート

ジャンボフレームはMTUサイズが9Kバイトまでのフレームであり、より少ないフレームを使用して同じデータを搬送するためネットワーク利用率が良くなる。 この機能の最大の利点とは伝送オーバーヘッドとホスト処理オーバーヘッドの削減である。 フレーム数が少ないと入出力の中断が少なくなる。 この機能はサーバ間転送に主として使用される。

MDI/MDIXサポート

イーサネット･コネクション･ブレードはRJ-45ポートに接続されたケーブルがクロスまたはストレートかを自動検出する。 端末用標準配線は媒体依存インターフェイス(MDI)であり、ハブおよびスイッチ用標準配線はMDIX (Media-Dependent Interface with Crossover)として周知である。

自動ネゴシエーション

自動ネゴシエーションによりイーサネット･コネクション･ブレードは動作モードを報知できる。 自動ネゴシエーションは2点間リンク部分を共有する2個のデバイスの間の情報交換さらにデバイスの伝送機能を最大限に活用するよう両デバイスを自動構成する手段となる。

2.1.1 MACアドレスによる機能

MACアドレス容量サポート

イーサネット・コネクション・ブレードはPG-SW112/PG-SW111に最大8K/16K個のMACアドレスをサポートする。イーサネット・コネクション・ブレードはシステム用に特定のMACアドレスをリザーブする。

静的MAC登録項目

MAC登録項目は受信フレームから学習する代わりにブリッジング・テーブルに装置時自身で入力できる。 これらのユーザー定義入力はエイジングとは無関係であり、リセットと再起動の際にも保持される。

自己学習型MACアドレス

イーサネット・コネクション・ブレードは受信パケットからのMACアドレス自動学習を可能にする。 MACアドレスはブリッジング・テーブルに保存される。

MACアドレス自動エイジング

所定時間MACアドレスからトラフィックが来ない場合このMACアドレスは無効化される。 このためブリッジング・テーブルはオーバーフローしない。

ポート・セキュリティ

ポート・セキュリティは未認証ユーザーがネットワークにアクセスするのを防止する。 この機能により当該ポートを通してネットワークにアクセスを承認されるデバイスに割当てるMACアドレス・リストを各ポートは学習できる。 このポートで受信されたパケットはすべて認証リストにあるソース・アドレスを持つ必要があり、これがない場合落とされる。 ポート・セキュリティはデフォルトではすべてのポートで無効化されているが、ポート毎に有効化できる。

アドレス・フィルタリング

このコネクション・ブレードはCPUポートに入るすべてのトラフィックのパケット・フィルターとなり、管理ネットワークに潜在的に転送またはルートされる。 パケット・フィルターは規則/パターンにより、あるパターンに合えばパケットを破棄し、あるパターンに合えばパケットを転送する2組のパターンから成る。

MACマルチキャスト・サポート

マルチキャスト・サービスは限定されたブロードキャスト・サービスであり、情報配信を1対多および多対1の接続により可能にする。 レイヤー2マルチキャスト・サービスでは1個のフレームが特定マルチキャスト・アドレスに宛てられ、そこからこのフレームのコピーが関連ポートに送信される。

2.1.2　レイヤー2+の機能

IGMP スヌーピング/MLD スヌーピング

IGMPスヌーピングはIGMPフレームがワークステーションからマルチキャスト･ルーターへイーサネット･コネクション･ブレードにより転送される際このフレームの内容を実行する。 フレームによりイーサネット･コネクション･ブレードはマルチキャスト･セッションのために構成されたワークステーションとマルチキャスト･フレームを送信しているマルチキャスト･ルーターを識別する。

ポート･ミラーリング

ミラー･ポートはプローブ･ポートで送信および受信されたパケットともにモニターする。 イーサネット･コネクション･ブレードでは複数のプローブ･ポートと1個のミラー･ポートをサポートする。 ミラー･ポートはすべてのプローブ･ポートのパケットをパケットが落とされるかに関わらずすべてモニターする。 プローブ･ポートとミラー･ポートはIBP管理機能から設定できる。 プローブ･ポートとミラー･ポートの設定時、すべてのパケットが正しく反映されるように両ポートを同速度に構成しなければならない。 物理ポートとポートチャネル･ポートをプローブ･ポートとしてもよい。

ブロードキャスト･ストーム制御

ストーム制御によりIPパケット･スイッチング量を制限できる。 理由は高速度と連続的トラフィックがネットワークをフラディングさせることがあるからである。 ストーム制御の仕組みはパケットがネットワーク上の他の部分をフラディングしないようにすることである。 ブロードキャスト、マルチキャストおよびユニキャスト転送速度がサポートされる。 ブロードキャスト、マルチキャストおよびユニキャスト･フレームに512pps(1秒当たりパケット数)の転送速度が可能である。 トラフィックは構成された転送速度を超えるとイーサネット･コネクション･ブレードで削除される。 ストーム制御はデフォルトで有効化されており、無効化できる。

802.1Q VLANタグ付け完全準拠

IEEE 802.1Qは仮想ブリッジLANのアーキテクチャ、VLANにより提供されるサービス、当該サービスの供給に関わるプロトコルとアルゴリズムを定義する。 この規格に含まれる重要な要件は必要とするサービス･クラス (QoS)のタグ値 (0-7)でフレームを印せることである。

リンクアグリゲーション

最大6個のメンバーポートを用いて1本の集約化リンクを定義し、単一のリンク集約化グループ(LAG)を形成できる。 これで可能になる機能：

- 物理リンク障害時の耐障害性保護
- より広い帯域接続
- 帯域粒度の向上
- 広帯域サーバ接続性

イーサネット･コネクション･ブレードは次の項目をサポートする：

- アップリンク･ポートでは 6 個のトランク･グループ、ダウンリンク･ポートでは 12 個のトランク･グループ。(ダウンリンク･ポート用LAGでは同一のイーサネット･コネクション･ブレード 接続された 1 台のサーバブレードで 2 個のポートを組合わせることもできる。)
- 構成可能規則による負荷分散： MACによるものとIPによるもの

LAGは全二重動作に設定された等速度のポートから構成される。LAGの性能を強化するため、フロー制御をLAGに対しても有効化できる。

© 2010 富士通テクノロジー･ソリューションズ

リンクアグリゲーションとLACP

LACPはリンク上のポイント通信を使用して動的にさまざまなリンクをアグリゲートし、現状のシステムペア間の最大アグリゲートを構成する。 LACPはシステム内でアグリゲート対象リンクへのポートの集約を自動的に決めたり、構成、結合、監視する。

リンク・レイヤーディスカバリープロトコル(LLDP)

LLDPのレイヤー2プロトコルであり、ネットワーク・デバイスがローカル・ネットワークにその識別番号と機能を報知することを可能にする。

IEEE 802.1ABLink Layer Discovery Protocol (LLDP)と呼ばれる確立された規格であり、拡張し続けるLAN構成上の課題にソリューションを与える。LLDPは具体的には、スイッチ、ルーター、ワイヤレスLANアクセス・ポイント等のイーサネット・ネットワーク・デバイスにネットワーク上の他のノードにこれらのデバイスに関する情報を広報し、これらのデバイスが発見する情報は保存できる標準的方法を定義する。 LLDPはすべての802準拠媒体で実行可能である。このプロトコルはデータ・リンク・レイヤーのみで実行され、異なるネットワーク・レイヤー・プロトコルを実行する2個のシステムが相互について学習することを可能にする。

アップリンク・グループ:

グループ定義は2つの独立する部分に分かれる。 外部/アップリンク・ポートではいわゆるアップリンク・セットに定義される。 次に続くグループ定義ではこれらのアップリンク・セットは外部接続を定義するために使用される。「アップリンク・セット」は、サーバ・グレード・グループを業務LANへ接続するためにポート・グループ定義で使用される1からnの外部（アップリンク）ポートの集合として定義される。 アップリンク・セットには2つのプロパティがある： ポート・バックアップとリンク・ステートである。

アップリンク・セットが生成されると、同時に2個のリンクアグリゲーションが生成される。 1つのリンクアグリゲーションはアクティブ用、他はバックアップ用である。 ポートはアップリンク・セットに参加し、自動的にアクティブなリンクアグリゲーションのメンバーとなる。 バックアップ・リンクアグリゲーションに参加するポートの割当はユーザで設定できる。

アップリンク・セットにポート・バックアップが有効化されると、フェイルオーバーが実行される。 すなわちアクティブLAGが停止するとバックアップLAGがアクティブなリンクになる。 アクティブLAGがアクティブに復帰すると、バックアップLAGはイナクティブに戻る。

アップリンク・セットにリンク・ステートが有効化されると、ダウンリンク伝搬が実行される。 すなわち、(ポート・グループやVLANポート・グループ等の)関連づけられたグループの ダウンリンク・ポートはアップリンク・ポートがリンク・ダウン中はリンク・ダウンする。

ポート・グループ

IBPのダウンリンク・ポートをポート・グループに組合わせることができる。 IBP機能ファームウェアによるイーサネット・コネクション・ブレードでは36個までのポート・グループを利用できる。 各ポート・グループには内部サーバ・ポート(INT1-INT36)を含むことができる。

ポート・グループには次の特長がある：

ポート・グループ毎に内部サーバポート(INT1-INT36)を含むことができ外部接続はアップリンク・セットに定義される(PG-SW112にはEXT37-EXT48、PG-SW111にはEXT37-EXT46）。 アップリンク・セットを含めなければいけないわけではない。 アップリンク・セットが無いグループは内部通信にのみ使用される。 グループ間の通信は不可であり、別のグループに見える一つのグループからのトラフィックも不可である。 デフォルトでは、サービスVLANとサービスLANによる以外は異なるポート・グループのポート間にトラフィックは無い。

ポート・グループのすべてのポートは同じ構成でなければならない。 ポート・グループのポートは固有のタグ無し/タグ付きVLANのメンバーである。

ポート・グループからポートを削除すると当該ポートは無効化され手動では有効化できない。 ポートがポート・グループに移動または割り当てされて参加すると、そのポートは再び有効化される。

© 2010 富士通テクノロジー・ソリューションズ

VLANポート･グループ

従来のポート･グループの特長と大きく異なる点はグループ化がVLANベースで定義され、VLANグループがアップリンク･セットを共有できることである。 同一のVLAN IDがあっても、異なるVLANポート･グループにあるVLANは異なるVLANである。

a) 内部 -> 外部 (ブレードサーバはパケットを送る):

ブレードサーバから受信され入ってくるタグ無しパケットはユーザ定義のグループVLANタグによりタグを付けられ、ポート･グループのアップリンク･セットへ転送される。 パケットはアップリンクをタグ付きパケットとして出て行き、VLAN タグはアップリンクで削除されない。 ブレードがタグ付きパケットを送り出していると、これらは破棄されるが、タグが定義されたサービス VLAN ID に等しい場合を除く。この場合、タグはサービス VLAN 定義に従い処理され、サービス VLAN アップリンク･セットへ転送される。

b) 外部 -> 内部 (ブレードサーバはパケットを受け取る):

IBP アップリンクで入ってくるタグ付きパケットはそのグループ VLAN タグ定義に従ってﾀﾞｳﾝﾘﾝｸ(ブレードサーバ)へ転送される。 このタグはダウンリンク･ポートで削除され、ブレードサーバはこのためタグ無しパケットを受信している。 VLAN グループにより定義されていない VLAN ID タグ付きパケットはアップリンクで落とされるが、サービス VLAN ID でタグを付けられたものは通す。これらのパケットはサービス VLAN グループの定義に従い処理される(次の節を参照) 。

ネイティブVLANオプションによるVLANポート･グループ

同じアップリンク･セットを共有するVLANポート･グループ･セットの中では、一つのVLANは「ネイティブVLAN」としてオプション定義可能である。 このためこのネイティブVLAN IDについてはアップリンク･ポートでのタグ付け動作が次のように変化する:

入ってくるタグ無しパケットは落とされずネイティブVLANIDによりタグを付けられVLANグループのすべてのﾀﾞｳﾝﾘﾝｸに転送される。 ネイティブVLAN IDでタグを付けられた受信パケットはアップリンクでは破棄される。 このアップリンク･セットに定義された他のVLANポート･グループのVLAN IDとも一致しないVLAN IDのタグ付きパケットは破棄される。 このVLANグループから送信されるすべてのパケットはIBPをタグ無しで送信し、ネイティブVLANタグは削ぎ落とされる。

制限事項:

- VLANポート･グループは内部ポートでは自身の間で中継しあってはならない。
- 2 個のVLANポート･グループが共通の外部ポートを共有する場合、異なるVLAN IDでなければならない。
- アップリンク･セットは外部ポートでは自身の間で中継しあってはならない。
- VLANポート･グループは内部ポートでも外部ポートでも「通常の」 ポート･グループを中継してはならない。
- VLANポート･グループのメンバーであるすべてのサーバブレードのLANポートはサービスVLANタグを除きVLANタグ付けを使用してはならない。

サービスLANとVLAN

サービスLANはサービスVLANと極めて類似する。 サービスLANはブレードからタグ付きパケットを受信するが、タグはアップリンク (外部ポート) を出るとき削ぎ落とされる。 アップリンク/外部ポートに入るタグ無しパケットはタグを付けられ、対応するダウンリンク/ブレードサーバへタグ付きパケットとして送られる。 アップリンク/外部ポートに入るタグ付き受信パケットは落とされる。

サービスVLANはブレードからサービスVLAN IDのタグ付きパケットを受け取り、タグ付きパケットとしてアップリンク (外部ポート) へ転送する。 アップリンク/外部ポートに入るサービスVLAN IDのタグ付き受信パケットはタグを付けられ、対応するダウンリンク/ブレードサーバ) へタグ付きパケットとして送られる。 (VLAN)ポート･グループとサービス(V)が内部ポート (ダウンリンク) で重複しうることに注意を要する。 ブレードまたはアップリンクから受信されたタグ無しパケットは(VLAN)ポート･グループの規則に従う必要がある。

異なるサービスVLANは同じアップリンク･セットを共有可能である。 サービスVLANのメンバーであるポートがサービスVLAN ID

(SVID)のタグ付きパケットを受信すると、受信されたこれらのタグ付きパケットはサービスVLANに基づいて転送される。 異なるVLAN IDのサービスVLANは内部ポートで重複しうる。 互いに素なアップリンク･セットによるサービスVLANは同じSVIDを持てる。 サービスVLANは内部ポートのみを定義してグループを形成し、アップリンク･セットを組合わせて外部接続を定義できる。

フェイルオーバー伝搬サポート

ブレードサーバには1個のデュアルポート･ネットワーク･インターフェイス･コントローラがあり、これはLANチーミング機能によるNIC管理プログラムを使用する場合冗長LANポートを提供する。 スイッチング時間を速め、冗長LANポートに素早くフェイルオーバーさせるように、フェイルオーバー伝搬機能がPG-SW111/PG-SW112から導入されアップリンク･ポート(物理ポートとポートチャネル･ポートを含む)は冗長LANポートの切替を速めることができるようになった。 フェイルオーバー条件にはリンク状態を含む。

ポート･バックアップ･サポート

ポート･バックアップはIBPの冗長アップリンク･ポートに対して提供されている。 ポート･グループが生成されると自動的に2個の集約グループが生成される。 集約グループの1つはアクティブ集約リンクとして、別の集約リンクはバックアップ集約リンクとして定義される。 アクティブ集約グループがリンク･ﾀﾞｳﾝとなると、バックアップ集約グループが伝送に使用される。 アクティブ集約グループがリンク･アップに戻ると、バックアップ集約グループはアクティブでなくなる。

2.1.3　イーサネット･コネクション･ブレードの管理機能

PRIMERGY BX900イーサネット･コネクション･ブレードはコンソール･ポートまたは、SNMP、TELNEtまたはHTTPプロトコルによりネットワークを介して管理できる。

管理操作で使用する各種のファイル：

a) BX900 イーサネット･コネクション･ブレードで使用する 3 種類のファイルがある:

- BootROMイメージ: 起動時にローダーが呼び出すイメージ。 POST(起動時自己診断) としても知られる。
- 設定ファイル： このファイルはシステム設定情報を保存する。
- オペコード： システム起動後に実行される、実行時イメージ。

b) フラッシュメモリの容量により、PRIMERGY BX900 は操作コードと BootROM イメージに各 2 個のコピー、設定ファイルでは 10 個のコピーのみサポートする。

c) イーサネット･コネクション･ブレードのデュアル機能モードは PRIMERGY BX900 サーバではサポートされており、ユーザーはイーサネット･コネクション･ブレードのコマンド･ライン･インターフェイス･コマンド機能の"スイッチ"か"IBP"に指定し、パワー･リサイクル後有効にできる。

管理ファイルの複製

PRIMERGY BX900は以上3種類のファイルを次の方法でコピーできる。

a) ローカルファイルからローカルファイルへのコピー: PRIMERGY BX900 は既存のローカル設定ファイルを別のローカルファイルにコピーできる。 既存ローカル操作コードの別のローカルファイルへのコピーは禁止される。

b) リモート TFTP/FTP サーバからローカルファイルへのコピー: PRIMERGY BX900 は設定ファイルまたは操作コードのリモート･サーバからローカルファイルへのダウンロードをサポートする。

c) ローカルファイルからリモート･サーバへ: PRIMERGY BX900 は既存のローカル設定ファイルのリモート･サーバへのアップロードをサポートする。

d) 実行コンフィグからローカルファイルへのコピー:

e) 実行コンフィグからリモート TFTP/FTP サーバへ.

f) ローカルファイルから実行コンフィグへのコピー。

g) リモート TFTP/FTP サーバから実行コンフィグへのコピー。

起動ファイルを選択する

デフォルト起動構成と実行イメージとして使用される起動ファイルとして10個の設定ファイルから1ファイル、2個の操作コードのコピーから1ファイルを選択でき、他の設定ファイルと操作コードはバックアップのために使用される。

構成をファイルに保存する

実行中の構成を今後使用するためにファイルに保存できる。 新たに保存されたこの設定ファイルを後で起動ファイルに選ぶことができる。 または、この保存された設定ファイルをリモート･サーバにアップロードしてバックアップできる。

プロビジョン

PRIMERGY BX900では設定ファイルを選択してシステムを構成できる。 システムを構成するには2つのタイミングがある： 起動時と実行時である。

a) 起動時: 設定ファイルを起動のために選択する。

b) 実行時: 新たな設定ファイルを選択して、システム実行中でもシステムを構成でき、システム再起動は必要だが自動的に適用される。 この機能はコマンド・ライン・インターフェイスのみで利用できる。

SNMPアラームとトラップ・ログ

システム・ログ・イベントには重大度コードとタイムスタンプが含まれる。 イベントはSNMPトラップとしてトラップ・レシーバ・リストに送られる。

SNMPバージョン1、バージョン2、バージョン3

UDP/IPプロトコルによる簡易ネットワーク管理プロトコル (SNMP) システムへのアクセスを制御するために、コミュニティー登録リストが定義され、この登録各項目はコミュニティー文字列およびアクセス特権から構成される。 SNMPセキュリティには読み出しのみと読み書きと2つのレベルがある。

ウェブによる管理

ウェブによる管理を用いてウェブ・ブラウザからシステムを管理できる。 システムには埋め込みウェブサーバ (EWS) が含まれ、これはHTML頁のサーバとなり、これを通してシステムを監視、構成できる。 システムはウェブによる入力を構成コマンド、MIB変数設定、他の管理関連設定に内部で変換する。

設定ファイルのダウンロードとアップロード

イーサネット・コネクション・ブレードの構成は設定ファイルに保存される。 設定ファイルはシステムとポート別のイーサネット・コネクション・ブレード構成を含む。 システムでは設定ファイル10個までがサポートされる。

スクリプト・ファイルの生成、ダウンロード、アップロード、適用

イーサネット・コネクション・ブレード構成の設定はテキストファイルとして保存され操作できるスクリプト・ファイルに保存できる。 スクリプト・ファイルには、設定ファイルがコマンド・ライン・インターフェイス・コマンドの集合として表記される。 スクリプト・ファイルはリモート・サーバとの間でダウンロード、アップロードともに可能であり、ダウンロードしたスクリプト・ファイルはコマンド・ライン・インターフェイス・コマンドによりシステムに適用できる。

TFTP/FTP 一般的なファイル転送プロトコル

イーサネット・コネクション・ブレードはTFTP/FTPによる起動イメージ、オペコード(実行時イメージ) 、設定ファイルのアップロードとダウンロードをサポートする。

遠隔監視

遠隔監視 (RMON) はSNMPを拡張したものである。(ネットワーク・イーサネット・コネクション・ブレード管理と監視を可能にするSNMPに対して)包括的なネットワーク・トラフィック監視機能を提供する。 RMONは現在および過去のMACレイヤー統計と制御オブジェクトを定義する標準MIBであり、実時情報をネットワーク全体から取得することを可能にする。

コマンド・ライン・インターフェイス

コマンド・ライン・インターフェイス(CLI)の構文と動作は業界標準に出来る限りに準拠する。 CLIは必須要素とオプション要素から構成される。 CLIはコマンドとキーワードを補完できるためユーザーを補助し、タイプを短くできる。

シスログ

シスログはリモート・サーバ・セットにイベント通知を送ることを可能にするプロトコルである。リモート・サーバにはイベント通知を保存でき、処理および直接対処できる。 重要なイベントの通知をリアルタイムで送信し、これらのイベントの記録を事後的に使用するため保存できるという複数の機構が実装されている。

SNTP

簡易ネットワーク･タイム･プロトコル (SNTP)精確なネットワーク･

イーサネット･コネクション･ブレードのクロック･タイム同期化をミリ秒精度で可能にする。 時間同期化はネットワークSNTPサーバが行う。 階層が時間ソースを確立する。

階層は参照クロックからの距離を定義する。 高階層であればあるほど(0に近づくほど)、クロックの精度は高い。 イーサネット･コネクション･ブレードはDHCPサーバから取得されたSNTPサーバの使用をサポートして情報が呈示されるとクロックを同期化する。

BOOTPクライアント

BOOTP(ブートストラップ･プロトコル)はデバイスが起動すると保存されたパラメータを持続的に使用する代わりに、ネットワークにIPアドレスを動的に割当てるために使用される。 BOOTPを使用するには、BOOTPサーバを立上げテーブルにデバイスのIPアドレスとMACアドレスを定義する必要がある。 デバイスが起動すると、BOOTP要求を送り出しBOOTPサーバからIPアドレスを取得し、プロトコル･スタックを開始する。

DHCP/DHCPv6クライアント

DHCP(動的ホスト構成プロトコル)はIPネットワーク上の個々のコンピュータにDHCPサーバから構成を展開する、特に、このサーバは各コンピュータが情報を要求するまでは個々のコンピュータについては精確な情報を持たない。 DHCPはBOOTPに基づいており、一部の下位互換性を保持する。 主な相違点は、BOOTPがサーバ･データベースにホスト情報を手動で予め構成するよう設計されている一方、DHCP は新たに接続されたホストにネットワーク･アドレスと構成を動的に割当てることを可能にする。 さらに、DHCPではリースメカニズムによりネットワーク･アドレスの復元と再割当てができる。

DNSクライアント

DNSプロトコルはホスト名をIPアドレスにマッピング可能な分散データベースであるドメイン･ネーム･システム(DNS)を制御する。 DNSをIBPに構成するとき、ホスト名を *ping, telnet, traceroute*等すべてのIPコマンドおよびTelnetサポート操作が可能なIPアドレスと代替できる。 ドメイン名を追跡するためIPではドメイン･ネーム･サーバというコンセプトが定義されており、これにはIPアドレスに対応させた名前のキャッシュ(すなわちデータベース)がある。 ドメイン名とIPアドレスを対応させるには、まずホスト名を定義し、ネットワークにあるネームサーバを指定してからDNSを有効化しなければならない。

DDNS クライアント

これでホスト名とそのIPアドレスを、指定されたDDNSサーバに対応づけてDNSを解決できる。

IPv6転送とIPv6サポート

IPv6とは"インターネット･プロトコルのバージョン6"を略記したものである。 IPv6はIETFが設計した次世代型プロトコルであり、現在のバージョンのインターネット･プロトコルである、IPバージョン4("IPv4")を置換する。 IPv6は利用可能なIPｖ4アドレスの数に限界があるといったIPｖ4の問題を解決する。 さらにルーティングやネットワークの自動構成等ではIPv4に多くの改善を追加する。 IPv6はIPv4を徐々に置換することが期待されており、推移期間中は両方が共存する。

管理用IPv6 IPアドレス

イーサネット･コネクション･ブレードのIPｖ６ IPアドレスはMACアドレスをもとに自動的に計算される。

管理ポート用デフォルト･ゲートウェイ

システムでは1個のデフォルト･ゲートウェイのみサポートされる。 インバンド管理インターフェイスまたはOut-of-band(OOB)管理インターフェイスのためにデフォルト･ゲートウェイを、*同時にではなく*、割当てることができる。 インバンド管理用ゲートウェイが設定されていれば、それはインバンド管理のみに有効である。 ゲートウェイをOut-of-band(OOB)管理にも設定しようとすると、インバンド管理用ゲートウェイがすでに設定されていて二回構成できないというエラー･メッセージが表示される。 Out-of-band(OOB)管理用ゲートウェイが設定さ

れていれば、それはOut-of-band(OOB)管理インターフェイスのみに有効である。 ここでもインバンド管理用ゲートウェイを構成しようとすると、対応するエラー･メッセージが表示される。

これら2個の管理ポートのうち1個をDHCPサーバからIPアドレスを取得するように構成すれば、DHCPサーバから取得されるデフォルト･ゲートウェイは既存のゲートウェイを上書きする。 すなわち、デフォルト･ゲートウェイは、DHCPサーバによりIPアドレスとデフォルト･ゲートウェイの割当が完了すれば、DHCPを使用するように構成される管理ポートには常に有効化される。

© 2010 富士通テクノロジー･ソリューションズ

2.1.4 セキュリティ機能

SSL

セキュア・ソケット・レイヤー(SSL)アプリケーション・レベルのプロトコルであり、非公開性、認証、データの完全性によりセキュリティが確立されたデータのやりとりを可能にする。 これは証明書および公開キーとシークレットキーを使用する。 現在はSSLバージョン3とTLSバージョン1がサポートされる。

SSH

セキュア・シェル(SSH)はプロトコルであり、イーサネット・コネクション・ブレードにセキュリティが確立した遠隔接続を可能にする。 現在はSSHバージョン1とバージョン2がサポートされる。 SSHサーバ機能によりSSHクライアントはイーサネット・コネクション・ブレードとセキュリティが確立された暗号化接続ができる。 この接続はインバウンドtelnet接続と同じ機能がある。 SSHはイーサネット・コネクション・ブレードの接続と認証にRSA公開キー暗号法を使用する。

ポートによる認証(802.1x)

ポートによる認証で外部サーバを介してポート毎にシステム・ユーザーを認証できる。 認証され許可されたシステム・ユーザーのみデータの送受信をできる。 ポートは拡張認証プロトコル (EAP)を使用するr遠隔認証ダイアルインユーザー・サービス(RADIUS) サーバを介して認証される。

RADIUSクライアント

RADIUSはクライアント/サーバ・ベースのプロトコルである。 RADIUSサーバはユーザー名、パスワード、アカウント情報等ユーザー毎の認証情報を含むユーザー・データベースを維持する。 詳細は"RADIUSのグローバル・パラメータを構成する"を参照のこと。

TACACS+ クライアント

TACACS+はイーサネット・コネクション・ブレードにアクセスするユーザーの認証に中央統合セキュリティ機能を提供する。 TACACS+はRADIUSおよびその他の認証プロセスとの一貫性を保持しつつも中央統合型ユーザー管理システムとなる。

LDAP クライアント

Lightweight Directory Access ProtocolすなわちLDAPはTCP/IPによるサービスのクエリーと変更に用いるアプリケーション・プロトコルである。 ディレクトリは同類の属性があるオブジェクトの集合を論理的で階層的に整理したものである。 最も馴染みのある例は電話帳であり、これにはアルファベット順に整理された名前 (人や組織) を含み、名前に住所と電話番号が付く。 その基本的設計により(とりわけこの要因により)LDAPは認証用に他のサービスにも使用されることがよくある。 イーサネット・コネクション・ブレードではLDAPはユーザー認証に使用される。

サービス妨害攻撃対策

サービス妨害攻撃はコンピュータの資源を本来のユーザーに利用できなくしようとする試みをいう。 ここでは、イーサネット・コネクション・ブレードは拡張対策機能を用いて本来のユーザーがその資源を利用できなくならないようにしている。

MACアドレス認証 (MACアドレス･フィルター)

ポート･ロックは特定MACアドレスのユーザーのみにアクセスを特定のポートに限定するためネットワーク･セキュリティを強化する。 当該アドレスは手動定義によるか適用ポートで学習される。 フレームがロックされたポートで発見され、フレーム･ソースMACアドレスがそのポートには関連付けられていないと、保護機構が発動される。

IPアドレス認証 (IPアドレス･フィルター)

管理IPアドレス･フィルターはイーサネット･コネクション･ブレードの構成変更を許可されるステーションを指定する。 5台までの管理ステーションをイーサネット･コネクション･ブレード管理用に選択できる。 1台以上の管理ステーションを定義しようとすると、IPアドレスにより定義された指定選択ステーションのみウェブ･マネージャ、Telnetｾｯｼｮﾝ、セキュア･シェル (SSH) またはセキュア･ソケット･レイヤー (SSL)でHTTPSの管理特権を許可される。

2.1.5 QOS機能

PRIMERGY BX900はDSCP(Differentiated Service Code Point)のCOSキューへのマッピングをサポートする。従って異なるDSCP値をもつパケットは異なるサービス用の別のCOSキューにスケジュール化できる。 DSCPの定義はTOS定義に下位互換性がある。

PRIMERGY BX900はこのためTOSからCOSキューへのマッピングもサポートする。 優先度が異なるパケットは異なるプライオリティのCOSキューにスケジュール化できる。

802.1pによるCoS

フレームを受信すると、イーサネット・コネクション・ブレードは802.1Qに定義されたVLAN IDにあるプライオリティ3ビットを処理してそのフレームのプライオリティを決定する。 フレームのプライオリティがわかると、そのプライオリティをフレームが転送されるべき各出力ポートで4つの出力キューのうち1個に利用できるよう対応づける。プライオリティ・マッピングと出力キューはWEB、CLI、またはSNMPインターフェイスを用いて自分で変更できることに注意されたい。 出力キューにあるフレームは次にスケジュール化アルゴリズムに従い転送される。

IP TOS/プレシデンス/DSCPベースのCoS

フレームを受信すると、イーサネット・コネクション・ブレードはパケットのIP TOS、IP Precedence、またはDSCPが所定値と一致するかを処理する。 真であれば、このフレームのクラスと関連付けられたポリシーを検査する。 ポリシーはユーザーが構成できる： DSCPフィールドを送る、落とす、マークする、プレシデンス・フィールドをマークする、またはこのクラスのフレームに特定の帯域を専用に割当てる。

アクセス・コントロール・リスト(ACLs)

パケット・フィルタリングはネットワーク・トラフィックや特定のユーザーまたはデバイスによるネットワーク使用を制限できる。 ACLはトラフィックがIBPを通過するとフィルターし、指定インターフェイスまたはVLANをパケットが通過するのを許可または拒否する。 ACLはパケットに適用する許可と拒否の条件をシーケンスに集めたものである。 パケットがインターフェイスで受信されると、IBPはパケットのフィールドを適用ACLと比較し、アクセスリストに指定された処理によりパケットが転送されるために必要な許可を得ているかを照合する。 最初の一致はIBPがパケットを許可するか拒否するかを決定する。 IBPは最初の一致で照合を止めるため、リストにある条件の順序は重要である。 条件に一致しないと、IBPはパケットを拒否する。 制限がない場合、IBPはパケットを転送し、それ以外の場合、IBPはパケットを破棄する。 IBPは転送するすべてのパケットを、VLAN内でブリッジ化されたパケットも含め、ACLを適用する。

これらのアクセス・リストはレイヤー2インターフェイスでサポートされる： ソース・アドレスを使用する標準IPアクセス・リストとソース・アドレスとターゲット・アドレスおよびオプションのプロトコル・タイプ情報を使用する拡張IPアクセス・リストである。 IBPは所与のインターフェイスに構成されたすべてのインバウンド機能と関連付けられたACLを照合し、ACLに登録された内容とパケットが一致するかに基づいてパケット転送を許可または拒否する。 このようにして、ACLはネットワークまたはネットワークの一部へのアクセスを制御するために使用される。

ACLは許可と拒否条件をシーケンスに集めたものである。 IBPはアクセス・リストにある条件でパケットを検査する。 最初の一致はIBPがパケットを許可するか拒否するかを決定する。 IBPは最初の一致で照合を止めるため、リストにある条件の順序は決定的に重要である。 条件に一致しないと、IBPはパケットを拒否する。

PRIMERGY BX900は次の種類のACLまたはIPアクセス・リストをサポートする：

- 標準IPアクセス・リストは一致検査にソース・アドレスを使用する。
- 拡張IPアクセス・リストは一致検査にソース・アドレスとターゲット・アドレスを使用し、より粒度の高い制御にはさらにオプションのプロトコル・タイプ情報を使用する。

標準ACLは初期ACLである。 標準ACLはIPパケットのソース・アドレスをACLに構成されたアドレスと比較してトラフィックを制御する。 標準ACLはIPパケットのソース・アドレスとターゲット・アドレスをACLに構成されたアドレスと比較してトラフィックを制御する。 規則はパケットの6個のフィールドまで照合するように構成できる： ソースIP、ターゲットIP、ソースL4ポート、ターゲットL4ポート、TOSバイト、プロトコル番号。

プライオリティ・キューの厳密なスケジュール化

WRRに加え、PRIMERGY BX900は厳密なスケジュール化もサポートし、プライオリティ・パケットが他のすべてのトラフィックに先んじて常に最初にサービスを受けること、他の3つのキューはWRRスケジュール化によりサービスを受けることを確保している。

WRR (荷重ラウンドロビン)

RIMERGY BX900WRRはWeighted Round Robin (WRR)によるスケジュール化をサポートする。 WRR キューイング・アルゴリズムではプライオリティの低いパケットが帯域を全く割当てられないことがないように、ネットワーク管理者により管理されるプライオリティ設定に影響を与えることなくサービスを受けることができる。

Differentiated Services

ネットワークリソースはトラフィック分類とプライオリティにより分割され、ネットワーク管理ポリシーに従い厳格なタイミングニーズのあるデータ処理を優先的に行う。 PRIMERGY BX900はDifferentiated Services(DiffServ)をサポートする。 DiffServはリソースリザベイションプロトコルを必要とせずにネットワーク・トラフィックにQoS処理を提供する方法である。 具体的には管理はネットワーク機器に次の内容を識別化するようプロビジョンを行う：ネットワークにおけるトラフィックのクラスおよびトラフィック・クラスが受けるQoS処理である。

DiffServはDiffServドメインを一貫してトラフィックを許容するか、DiffServドメインを一環してトラフィックを伝送するか、さらにネットワーク・ノード内で帯域を保証するかを制御する。 許容、伝送および帯域の制御により、ポリシーによるサービスの範囲が定められる。

DiffServを構成するには3個のキーQoS構築ブロックがある。 クラス、ポリシー、サービスである。

DiffServを構成するには3個のキーQoS構築ブロックがある。 クラス、ポリシー、サービスである。

- Class
- Policy
- Services.

クラスの構成では、特定トラフィック・クラスの一致基準をユーザーが指定する。 イーサネット・コネクション・ブレードに提供される基準には次がある：

- Destination MAC address,
- Destination IP address,
- Destination layer 4 port,
- IP DSCP,
- IP Precedence,
- IP TOS,
- Protocol,
- Source MAC address,
- Source IP address,
- Source layer 4 port,
- Any.

© 2010 富士通テクノロジー・ソリューションズ

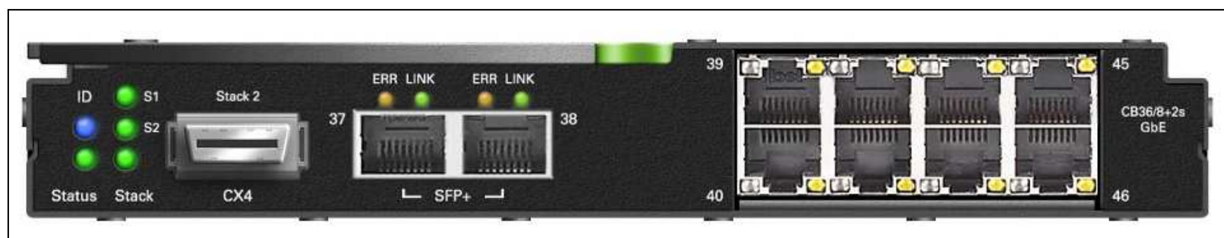
2.2 ハードウェアの説明

2.2.1 イーサネット･コネクション･ブレードのポート構成

PRIMERGY BX900イーサネット･コネクション･ブレードは、a) ネットワーク接続用にPG-SW111、8個のギガビット･イーサネット･ポートおよび2個の10ギガSFP+イーサネット･ポートPG-SW111、b) ネットワーク接続用にPG-SW112、8個のRJ45ギガビット･イーサネット･ポートと4個のSFPギガビット･イーサネット･ポートを含む。PRIMERGY BX900ブレードサーバ管理MMBモジュールの接続用に1個のOut-of-Band管理イーサネット･ポートがある。

a)PG-SW111用の物理ポート

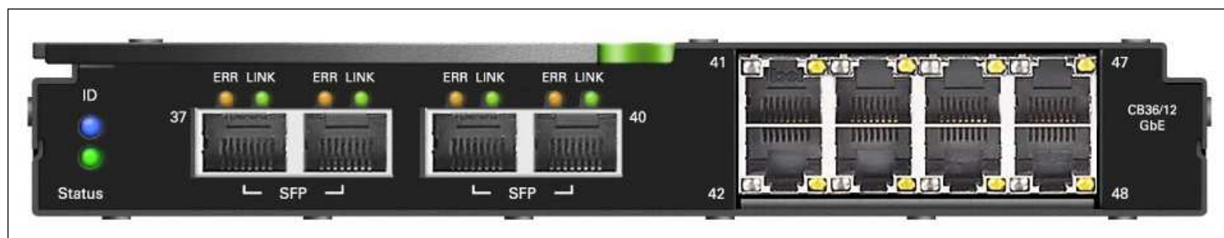
- 36個の1ギガビット･ダウンリンク･ポート
- 8個のアップリンク･ポート用1ギガビットRJ45ポート
- 2個のアップリンク用10ギガビットSFP+ポート
- 最大8個のデバイスまでスタック可能な2個のHiGig/HiGig+ポート。 このうち1個はシステム中央部の内部スタック用であり、もう1個は外部スタック用である。



図： PRIMERGY BX900 GbEコネクション･ブレードの 36/8+2 スタック (PG-SW111) 前面

b)PG-SW112用の物理ポート

- 36個の1ギガビット･ダウンリンク･ポート
- 8個のアップリンク･ポート用1ギガビットRJ45ポート
- 4 個のアップリンク用1ギガビットSFPポート



図： PRIMERGY BX900 GbEコネクション･ブレードの 36/12 スタック (PG-SW112) 前面

8個のRF45ギガビット･イーサネット･ポートは10、100、または1000 Mbpsで動作できる。 これらのポートはネゴシエーション、二重モード(半二重または全二重)、およびフロー制御をサポートする。 サーバに接続する36個のダウンリンク用1ギガビット･イーサネット･ポートは1000Mbps、全二重、フロー制御のみで動作可能である。

2.2.2 イーサネット･ポート

アップリンク･ポート

8個の外部RJ45ポートはIEEE 802.3x自動ネゴシエーションによる速度、二重モード、フロー制御をサポートする。 ポートは10Mbps、100Mbps、または1000Mbps、半二重、全二重で動作し、データの流れを制御してバッファーをオーバーフローさせない。 アップリンク･ポートはCat 5ツイストペア･ケーブルを使用して最長100m(328フィート)まで離れたIEEE 802.3ab 1000BASE-T準拠機器に接続できる。 これらのポートは自動MDI/MDI-X機能があり、全ての接続をストレート･ケーブルでも行える。 さらに、PG-SW112のSFPポートはシングル･モードとデュアル･モードをサポートし、PG-SW111の10ギガ･ポートは標準SFP+に準拠する。

注 – 自動ネゴシエーションを使用する際は、速度、伝送モード、フロー制御はこの機能が接続デバイスでもサポートされる場合自動的に設定される。 これ以外の場合各項目を接続毎に手動で構成できる。

注 – 自動MDI/MDI-Xピンアウト構成のために有効化されなければならない。

内部ポート

イーサネット･コネクション･ブレードはシャーシのサーバブレードに接続する36個の内部1000BASE-Xイーサネット･ポートも含む。 これらのポートは1000Mbps、全二重に固定されている。

2.2.3 LEDの状態

フロント・パネルには発行ダイオード (LED)があり、リンク、イーサネット・コネクション・ブレード診断の状態を示す。

ポートLED

アップリンク毎に2個のLEDインジケータがある。

RJ45:

LED	色	意味
LED-A (速度)	オレンジ	ポート・リンク速度1000Mbps
	緑	ポート・リンク速度100 Mbps
	消灯	ポート・リンク速度10 Mbps
LED-B (リンク/動作)	緑	ネットワーク・リンク
	緑点滅	ネットワーク動作中
	消灯	ネットワーク・リンクが無いまたはポートが無効

SFP:

LED	色	意味
リンク	消灯	ネットワーク・リンクが無いまたはポートが無効
	緑	SFPトランシーバ・リンクの状態
	緑点滅	SFPトランシーバ　アクティブ状態
ERR	消灯	SFPエラー無し
	オレンジ	SFPトランシーバ　エラー
	オレンジ点滅	SFPモジュールがサポートされていない

SFP+:

LED	色	意味
リンク	消灯	ネットワーク・リンクが無いまたはポートが無効
	緑	SFP＋トランシーバ・リンクの状態
	緑点滅	SFP＋トランシーバ　アクティブ状態
ERR	消灯	SFP＋エラー無し
	オレンジ	SFP＋トランシーバ　エラー
	点滅オレンジ	SFP＋モジュールがサポートされていない

© 2010 富士通テクノロジー・ソリューションズ

汎用LED

1個のイーサネット･コネクション･ブレード･システムLEDがあり二つの機能があり、MMBによりエラー･ｽﾃｰﾀｽ通知とブレード識別を制御される。 異なる点滅周波数が使用され異なる機能を示す。 識別とエラー通知の二機能があり、エラー通知より識別が優先される。

LED	色	意味
ID	青	コネクション･ブレードを識別する
	消灯	通常
Status	緑	電源投入状態
	点滅オレンジ	コネクション･ブレードの障害
	消灯	電源遮断状態
S1	緑	内部スタック･ポート1のリンク
	緑点滅	内部スタック･ポート1の動作
	消灯	スタック･ポート1のリンク無し
S2	緑	外部スタック･ポート2のリンク
	緑点滅	外部スタック･ポート2の動作
	消灯	スタック･ポート2 のリンク無し
Stack	黄	コネクション･ブレードはスタック･マスター
	黄点滅	コネクション･ブレードがマスター機能を果たせない
	緑	コネクション･ブレードはスタック･スレーブ
	緑点滅	マスター選択中
	消灯	コネクション･ブレードがスタックに無い

2.2.4　サポートされるSFP+とSFPのベンダー一覧表

サポートされるSFPモジュール：

ベンダー	製造番号P/N
フィニサー社	FCLF-8521-3
フィニサー社	FTLF8524P2BNV

サポートされるSFP＋ モジュール：

ベンダー	製造番号P/N
オプネクスト社	TRS2000EN-S002
フィニサー社	FTLX8571D3BCL

2.3 機能と利点

2.3.1 接続機能

- 36個の内部ギガビット・ポートでサーバ・カードの容易なネットワークへの統合が可能。
- 8個の外部1000BASE-Tギガビット・ポートが企業ネットワークへのアップリンクを提供。
- 4個のSFPギガビット・ポートが企業ネットワークへのアップリンクを提供。 (PG-SW112)
- 2個のSFP＋ 10ギガビット・ポートが企業ネットワークへのアップリンクを提供。 (PG-SW111)
- 外部ポートの自動MDI/MDI-Xサポートによりすべての接続をストレート・ケーブル (自動ネゴシエーションが有効化された状態で) でも可能。
- 自動ネゴシエーションはポート毎に最適速度 (10、100、または1000Mbps)と通信モード (半二重か全二重) の自動選択を可能にする。ただし接続機器にこの機能がある場合。これ以外の場合、ポートは手動構成できる。
- IEEE 802.3adギガビット・イーサネット準拠によりベンダーの規格準拠ネットワーク・カードとスイッチと互換性が保たれる。

2.3.2 性能

- トランスペアレントブリッジング
- 転送モード： ストアーアンドフォワード
- 帯域： 152Gbps (PG-SW111) / 96Gbps (PG-SW112)
- スイッチング遅延： 64バイト・フレームでは平均8us
- スイッチング・テーブル、8K (PG-SW112) /16K (PG-SW111) MAC アドレス・エントリ
- 平均故障間隔 (MTBF): 175699 時間

2.3.3 管理

- Telnet、SNMP/RMON、ウェブ・ベースのインターフェイス
- ｲﾝﾊﾞﾝﾄﾞ管理インターフェイス上のVLANサポート、ポート・ベースまたは802.1Q VLANタグ付けによる
- 4本のキューでサポートされるQoS
- IGMP(インターネット・グループ管理プロトコル) /MLDスヌーピングによるフィルタリングに基づくマルチキャスト・スイッチング
- ブロードキャスト・ストーム抑制
- ポート・ミラーリング
- リンクアグリゲーション
- ユーザー名とパスワード、SNMPコミュニティー名による管理アクセス・セキュリティ

2.4 表記規則

この手順書で使用される記号やフォントの意味を次に定義する。

⚠ 要注意	この記号を付された文には特に注意を払うこと。 この警告に従わないと人命への危険、システムの破壊、データ損失に至るおそれがある。
引用符””	章の名前、強調される用語に使う。
i 注意:	この記号は補足的情報、備考、ヒントとともに用いられる。

2.5 この手順書の対象ユーザー

この手順書はネットワーク接続の設置と構成を担当する技術要員を対象とする。 この手順書にはイーサネット･コネクション･ブレードを構成するために必要な情報がすべて掲載される。

2.6 テクニカル･データ

電気系データ

運転電圧	+12 VDC @ 2.5 A 最大 (PG-SW112) +12 VDC @ 3.5 A 最大 (PG-SW111)
最大電流	7.52 A max @ 3.3 VDC 11.8 A max @ 2.5 VDC 24 A max @ 1.25 VDC 7.76 A max @ 1 VDC

国内および国際規格

製品の安全性	IEC 60950 / EN 60950 / UL 60950, CSA 22.2 No. 950
電磁両立性 干渉エミッション 高調波電流 フリッカー 干渉耐性	FCC クラスA VCCI クラスA AS / NZS 3548クラスA EN 55022 EN 61000-3-2 JEIDA EN 61000-3-3 EN 55024 EN 61000-4-2/3/4/5/6/8/11 BSMI CNS 13438
EU指令によるCE認証:	73/23/EEC (低電圧指令) 89/336/EEC (電磁両立性)

寸法

長さ (L)	276.24 mm
幅 (W)	192.63 mm
高さ (H)	28.04 mm

環境条件

環境クラス3K2 環境クラス2K2	DIN IEC 721 パート3-3 DIN IEC 721 パート3-2
温度: – 稼働時 (3K2) – 輸送中 (2K2)	 0 ° C .... 50 °C -40 °C .... 70 °C
湿度	10 ... 90%

稼動中の結露は必ず回避すること。

© 2010 富士通テクノロジー･ソリューションズ

3 ネットワーク計画

3.1 IBPの初歩

インテリジェント・ブレード・パネル (IBP)はPRIMERGY BX900ブレードサーバをネットワーク基盤に接続するための簡易なイーサネット・インターフェイス・オプションとなる。 ネットワークに接続するために要求される管理要求度とネットワークスキルは最小限にとどめてある。 IBPの構成オプションの数と種類は制限されており初期セットアップの複雑性を軽減し上流ネットワーク機器への影響を最小限にする。

IBPは同一マルチリンク・サーバをネットワークに接続するのと基本的管理作業が同じである。 ブレードセンターのサーバブレード最大10台への接続は同一サーバをネットワークに接続するくらい簡単にできる。

IBPのデフォルト・ネットワーク構成は単一のタグ無し仮想ローカル・エリア・ネットワーク (VLAN) から成る。 アップリンク・ポートのすべてが静的リンクアグリゲーション・グループ (LAGまたはトランク・グループ) に集約され、シスコのイーサーチャネル技術と完全に互換性がある。 この構成はスパニング・ツリー・プロトコルの必要性を無くし、アップリンク・ポートが単一リンクとして機能するのでネットワーク・ループを防止できる。

IBPによりネットワークの信頼性が改善される。 各ポート・グループのすべてのアップリンク・ポートは静的LAGに参加するので、1本のリンクが障害を起こしても、現在のトラフィックは他のリンクにリダイレクトされる。

IBPソフトウェアで銅TXアップリンク・ポートも各リンクの速度 (10/100/1000Mbps)、全二重、フロー制御設定(デフォルト設定)を自動ネゴシエートできる。 手動でこれらのポートの特性を指定値に固定もできる。 各ポート・グループのすべてのアップリンク・ポートは同じポート特性で構成しなければならない。

ネットワーク・アダプタのチーミングがサーバ・ブレード・イーサネットNICで構成され、サーバはブレード・サーバ・シャーシ内で複数のIBPへの冗長リンクを保持でき、信頼性が強化される。 L2フェイルオーバー・オプションによりIBPは外部アップリンクがすべて無効なときはサーバブレード・ポートを無効化できます。 このためネットワーク・アダプタのチーミング・ソフトウェアはブレード・サーバ・シャーシの他のIBPにフェールオーバーする。

3.2 用途例

イーサネット・コネクション・ブレードはネットワークを統合するよう設計されており、ネットワーク・コアはサーバシャーシとワークグループ・スイッチの間に広帯域接続を提供できる。 この節でその一部の主要用途を説明する。

3.2.1 バックボーン接続

IBPは高速ギガビット・イーサネット・リンクによりネットワーク・バックボーンまたは他の主要サイトへ接続でき、全体の帯域と処理能力が増大する。

IBPのアップリンク・セットは企業バックボーン、インターネット、他のサーバへの広帯域接続を可能にする。

© 2010 富士通テクノロジー・ソリューションズ

3.2.2 IBP接続を確立する

IBPはどんなサーバブレード・グループでも別個のブロードキャスト・ドメインに整理するために使用できるポート・グループをサポートする。 ポート・グループはソース・グループにブロードキャスト・トラフィックを制限し、大規模ネットワークのブロードキャスト・ストームを解消できる。 ポート・グループ間の通信は不可であり、別のグループに見える一つのグループからのトラフィックも不可能である。 このためよりセキュアできれいなネットワーク環境が提供される。

ポート・グループ内のトラフィックは受信されると送信される、すなわち、VLANトランスペアレントである。

© 2010 富士通テクノロジー・ソリューションズ

4 ネットワーク接続を確立する

イーサネット・コネクション・ブレードはシステム内に取付けられたサーバボードを共通スイッチ・ファブリックに接続するとともに、外部ポートをIEEE 802.3ab準拠の外部機器にアップリンクするように提供する。 ほとんどの用途ではイーサネット・コネクション・ブレードの外部ポートはネットワーク・バックボーンにある他のスイッチに接続することができる。 さらにPCやサーバのギガビット・イーサネット・ネットワークにも直接接続できる。

4.1 1000BASE-T機器に接続する

IBPのデータ・ポートは10Mbps、100Mbps、1000Mbps、全二重、半二重で動作し、さらにシード、二重モード、フロー制御の自動ネゴシエーションをサポートできる。 IBPのデータ・ポートはいずれもどのサーバまたはワークステーション、または別のIBPやルーター等ネットワーク機器へのアップリンクでも接続できる。 1000BASE-T規格は最大長100m(328フィート)までの接続にCat5ツイストペア・ケーブルを4対使用する。



1000Mbps接続ではケーブルがIEEE 802.3ab 1000BASE-Tに準拠して設置できるか試験する必要がある。 詳細は"1000BASE-Tケーブル要件"を参照されたい。

1. ネットワークを構成する機器の準備をする。 1000Mbps 接続には、サーバとワークステーションに 1000BASE-T ネットワーク・インターフェイス・カードが取付けられていることを確認すること。 他のネットワーク機器は IEEE 802.3ab 1000BASE-T 規格に準拠する RJ45 ポートがなければばならない。

2. RJ45 プラグが両端にあるシールドまたは非シールド・ツイストペア・ケーブル (ストレートまたはクロスオーバー) を準備する。 1000Mbps ギガビット・イーサネット接続用の 100Ω Cat5 (Cat5e 以上を推奨)ケーブルを使用すること。
3. ケーブルの一端を他の機器の RJ45 ポートに接続し、他端は IBP で利用できる RJ45 ポートに繋ぐ。 RJ45 プラグを差し込む際、プラグにあるタブがカチッとはまり、正しく固定されることを確認する。



RF45ポートに電話用ジャックコネクタを差し込まないこと。 イーサネット・コネクション・ブレードを損傷することがある。 必ず、FCC規格準拠のRJ45コネクタ付きツイストペア・ケーブルのみ使用する。



1000Mbps接続にはケーブルの4対すべてを接続しなければならない。 自動ネゴシエーションが有効化されている場合、1000BASE-Tポートは自動MDI/MDI-X 機能をサポートする、すなわちストレート機器であっても10Mbps、100Mbps、または1000Mbpsの速度をサポートできる。 ツイストペア・ケーブル1本は100m(328フィート) を超えないようにする。 自動ネゴシエーションは自動MDI/MDI-Xのサポートには有効化されなければならない。

4.2 1000BASE-Tケーブル要件

100BASE-TXで使用するすべてのCat5UTPケーブルなら4対ラインすべてが接続されていれば1000BASE-Tにも使用できる。 しかしすべての基幹接続または新たなケーブルの設置の場合、Cat5e (拡張Cat5)ケーブルを使うこと。 Cat5e規格はCat5のみに推奨されるテスト・パラメータを含む。従って、1000BAST-Tを実行するために既存Cat5ケーブルを準備する際最初に行うべきことは、IEEE 802.3ab規格準拠性を確かめるために、設置されたケーブルを単にテストする。

4.2.1 既存Cat5 ケーブルのケーブル・テスト

敷設済みのCat5ケーブルは減衰、近端漏話(NEXT)、遠端漏話(FEXT)のテストに合致しなければならない。 このケーブルテスト情報はANSI/TIA/EIA-TSB-67規格に指定されている。 さらに、反射損失と等レベル遠端漏和(ELFEXT)のテスト・パラメータにも合致しなければならない。 これらのテストはANSI/TIA/EIA-TSB-95冊子"100Ω4対Cat5ケーブルの追加的伝送性能ガイドライン"に指定されている。

敷設されたケーブルをテストする際、IBPと端末機器の間のすべてのパッチケーブルも含むこと。

4.2.2 既存Cat5 ケーブルを 1000BASE-Tに調整する

既存のCat5敷設ケーブルが1000BASE-Tのテスト・パラメータの一つに不合致な場合、問題を修正するために適用できる3つの基本措置がある。

1. Cat5 パッチケーブルを高性能 Cat5e ケーブルと交換する。
2. リンクに使用されるコネクタ数を減らす。
3. リンクのコネクタの一部を抜いてから再び接続してみる。

4.2.3 1000BASE-Tのピン割当て

1000BAST-Tポートは自動MDI/MDI-Xをサポートするので、PCやサーバまたは他のスイッチとのすべてのネットワーク接続にストレート・ケーブルを使用できる。 (自動ネゴシエーションはMDI/MDI-Xをサポートするには有効化されなければならない。)

次表は1000BASE-T MDIとMDI-Xポートのピン配列を示す。

これらのポートではワイヤの4対すべてが接続されることが要件である。 1000Mbps接続ではワイヤの4対すべてが送受信の両方に使用されることに注意する。

1000Mbps接続には100ΩCat5かCat5eの非シールド・ツイストペア (UTP)またはシールド・ツイストペア(STP) ケーブルを使用する。 ツイストペア接続の長さが100m(328フィート)を超えないようにする。

ピン	MDI信号名	MDI-X信号名
1	送信データプラス(TD1+)	送信データプラス(TD2+)
2	受信データマイナス（RD1-)	受信データマイナス（RD2-)
3	送信データプラス(TD2+)	送信データプラス(TD1+)
4	送信データプラス(TD3+)	送信データプラス(TD4+)
5	受信データマイナス（RD3-)	受信データマイナス（RD4-)
6	受信データマイナス（RD2-)	受信データマイナス（RD1-)
7	送信データプラス(TD4+)	送信データプラス(TD3+)
8	受信データマイナス（RD4-)	受信データマイナス（RD3-)

ピン	MDI信号名	MDI-X信号名
1	送信データプラス(TD1+)	送信データプラス(TD2+)
2	受信データマイナス（RD1-)	受信データマイナス（RD2-)
3	送信データプラス(TD2+)	送信データプラス(TD1+)
4	送信データプラス(TD3+)	送信データプラス(TD4+)
5	受信データマイナス（RD3-)	受信データマイナス（RD4-)
6	受信データマイナス（RD2-)	受信データマイナス（RD1-)
7	送信データプラス(TD4+)	送信データプラス(TD3+)
8	受信データマイナス（RD4-)	受信データマイナス（RD3-)

表；1000BASE-Tのピン配列

© 2010 富士通テクノロジー・ソリューションズ

5　　イーサネット·コネクション·ブレードを構成する

この節はイーサネット·コネクション·ブレードの開梱、設置、ケーブル接続について説明する。

5.1　　概　要

イーサネット·コネクション·ブレードはPRIMERGY BX900ブレードサーバに挿入され、プロセッサ·ブレードは18枚までイーサネット·コネクション·ブレードは8台まで統合できるサーバモジュールである。

梱包の内容

イーサネット·コネクション·ブレードを開梱する際、次の品目が含まれていることを確認する。

- **イーサネット·コネクション·ブレード**

イーサネット·コネクション·ブレードの開梱

イーサネット·コネクション·ブレードを開梱する手順:



イーサネット·コネクション·ブレードを開梱する前に、梱包内容を検査して損傷が明らかにあれば直ちに報告する。

静電で損傷しやすいデバイス用ストラップは同梱されてはいないが、次から先の手順を行う際はストラップを着用したほうがよい。

1. **容器を開く。**
2. **イーサネット·コネクション·ブレードを容器から注意して取り出し、安全で清潔な表面に置く。**
3. **梱包資材をすべて取り去る。**
4. **イーサネット·コネクション·ブレードに損傷がないか点検する。 損傷があれば直ちに報告する。**



この資料の図解は実物イーサネット·コネクション·ブレードとシャーシとは若干異なる場合がある。

5.2　イーサネット･コネクション･ブレードを接続する

イーサネット･コネクション･ブレードを構成する前に、PRIMERGY BX900ブレード･サーバのコンソール･ポートをイーサネット･コネクション･ブレードに接続しなければならない。 PRIMERGY

BX900ブレード･サーバのコンソール･ポートをイーサネット･コネクション･ブレードに接続する手順は以下の通りである：

1. イーサネット･コネクション･ブレードを取付ける

コンソール･モニターに MMB アプリケーションのログイン画面が表示される。

イーサネット･コネクション･ブレードの起動画面が表示される。

```
                    Welcome to Management Blade 1.30J


<Username>:
```

2. 支給されたユーザー名とパスワードを入力する。 コンソール･メニューが表示される。

```
                    Welcome to Management Blade 1.30J


<Username>:admin
<Password>:*****


+---------------------------------------------------------------------------+
|                          Console Menu                  page_root
+---------------------------------------------------------------------------+
(1) Management Agent
(2) Emergency Management Port
(3) Console Redirection
(4) TFTP update
(5) Logout
(6) Reboot Management Blade
(7) System Information Dump
(8) Command Line Interface
(9) Account Management
Enter selection: 3
```

© 2010 富士通テクノロジー･ソリューションズ

3. (3) Console Redirection を選択する。 Console Redirection Table (コンソール・リダイレクション・テーブル)が表示される。

```
+--------------------------------------------------------------------------------+
|           Console Redirection Table                              page_3
+--------------------------------------------------------------------------------+
(1) Console Redirect Connection Blade
(2) Set Return Hotkey , Ctrl+(a character) : Q
(3) Set Console Redirection Timeout            : 900
Enter selection or type (0) to quit: 1
```

4. (1) Console Redirection Connection Blade を選択する。 Console Redirect Connection Blade が表示される。

```
+--------------------------------------------------------------------------------+
|           Console Redirect Connection Blade                      page_3_1
+--------------------------------------------------------------------------------+
(1) Console Redirect Connection Blade-1
(2) Console Redirect Connection Blade-2
Enter selection or type (0) to quit: 1
```

5. リダイレクトするコネクション・ブレードを選択する。 次にEnterを押してコンソールがリダイレクトされたかを確認する。

```
Press <Ctrl+Q> Return Console Menu


(BX900-CB1)#
```

© 2010 富士通テクノロジー・ソリューションズ

5.3 イーサネット･コネクション･ブレードの起動と構成

イーサネット･コネクション･ブレードを構成する際イーサネット･コネクション･ブレードのアーキテクチャを理解しておくことが重要である。 イーサネット･コネクション･ブレードには2種類のポートがある。 一つはイーサネット･コネクション･ブレードとPRIMERGY BX900ブレード･サーバとのインターフェイス用、もう一つはPRIMERGY BX900ブレード･サーバを外部ネットワークに接続するための普通のイーサネット･ポートである。

PRIMERGY BX900ブレード･サーバはPRIMERGY BX900ブレード･サーバの (管理ボード) MMBとは内部ポートと呼ばれる36個の内部ポートにより接続される。 内部ポートのリンク最高速度はポート毎に1ギガビットである。 ポート構成IDはg1からg36までである。 イーサネット･コネクション･ブレードを外部ネットワークと接続するために、外部ポートと呼ばれる、8個のPHYベース･ポート、4個の1ギガビットSFPポートまたは2個のSFP+10ギガビット･ポート (プラットフォーム･タイプにより異なる)がある。

内部ポートと外部ポートのデフォルト構成は次の通りである：

外部ポート	
意味	初期設定
フロー制御	オフ (入口では無効化されている)
バック･プレッシャ	オフ (入口では無効化されている)
自動ネゴシエーション	有効

表； 外部ポートのデフォルト構成

内部ポート	
意味	初期設定
速度と二重自動ネゴシエーション	1ギガビット フルスピード
フロー制御	無効
フロー制御の自動ネゴシエーション	無効

表；外部ポートのデフォルト構成

© 2010 富士通テクノロジー･ソリューションズ

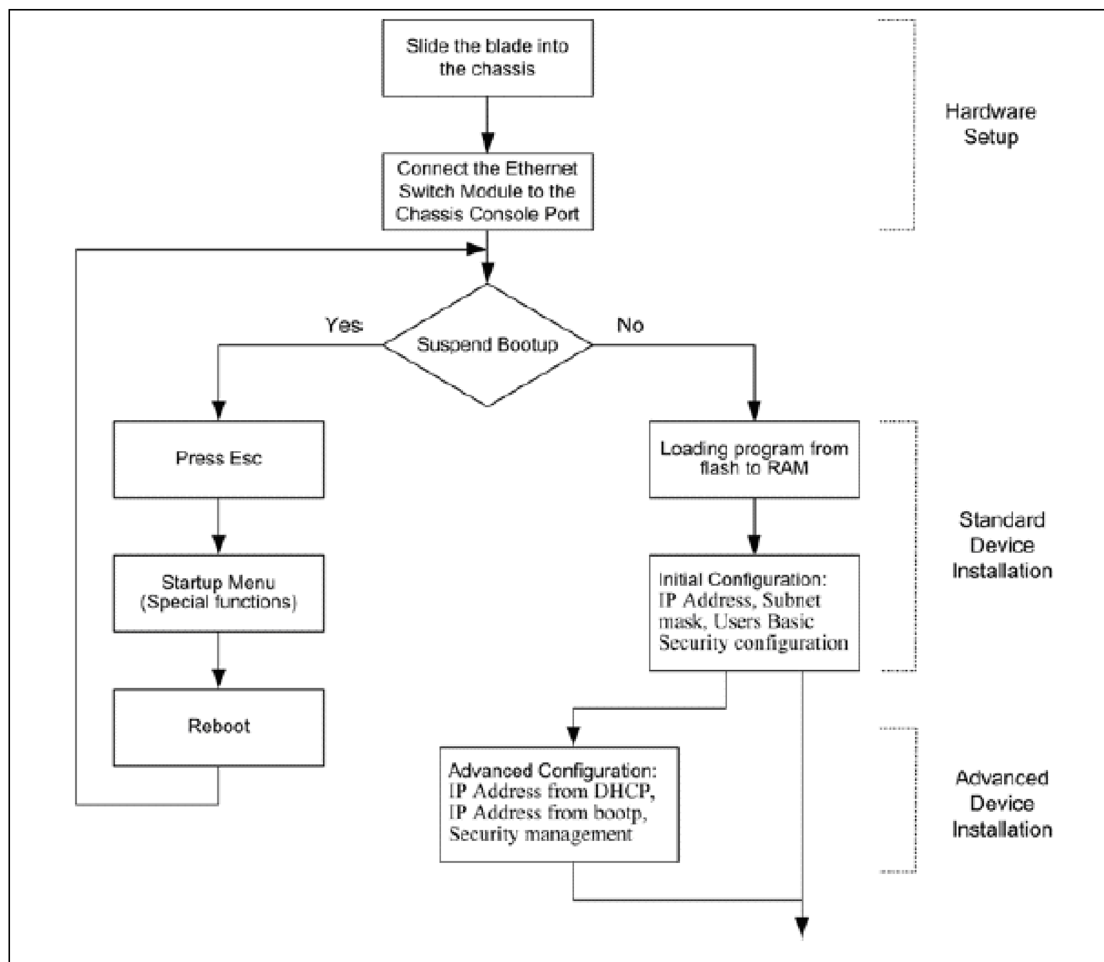


図: 設置と構成作業の流れ

5.4 端末を構成する

デバイスを構成するには、ステーションは端末エミュレーション･ソフトウェアを実行していなければならない。 イーサネット･コネクション･ブレードが正しく取付けられ、シャーシのシリアルポートに接続されていることを確認する。 端末エミュレーション･ソフトウェアは次のように設定する: PRIMERGY BX900マネジメント･ブレードのシリアルポートに接続し、コンソール･リダイレクト機能を使用してイーサネット･コネクション･ブレードにコンソールからアクセスできるようにする。



1. データ形式をボーレート 115200、データビット 8、ストップビット 1、パリティ無しに設定する。
2. フロー制御を無しに設定する。
3. プロパティで、エミュレーション･モードのために VT100 を選択する。
4. 機能、矢印、Ctrl キーに端末キーを選択する。 この設定は端末キー用である (ウィンドウズキーとは異なる) 。

端末からイーサネット･コネクション･ブレードにアクセスするには次の手順を踏む:

1. 端末をマネジメント･ブレードのシリアルポートに接続する。
2. マネジメント･ブレードのコンソール･リダイレクト機能を使用して必要なイーサネット･コネクション･ブレードへのアクセスを得る。
3. 何回か<Enter>キーを押して端末接続が成功したか確認する。

© 2010 富士通テクノロジー･ソリューションズ

5.5 デバイスを起動する

イーサネット・コネクション・ブレードをローカル端末に繋ぐとイーサネット・コネクション・ブレードは電源投入時自己診断 (POST) を行う。 電源投入時自己診断はデバイスが初期化される度に実行され、ハードウェア部品を検査してデバイスの起動が完了する前にデバイスが完全に機能するかを同定する。 重要な問題が検出されると、プログラム・フローは止まる。 端末にPOSTが診断結果の成功か失敗を表示する。

デバイスが起動すると起動時診断はまずデバイス・メモリの可用性を調べてから、起動を継続する。 次の画面はPOST表示例である。

```
------------ Performing Power-On Self Tests (POST) --------------
   System SDRAM Test..........···············.........PASS
   CPU Self Test......................·····················.PASS
   UART Loopback Test.................···············..PASS
   Flash Memory Initialize............···················.PASS
   Flash Memory Checksum Test.........·········...PASS
   PCI Bus Initialize and Test........···················PASS
   System Timer Test..................···················..PASS
   I2C Bus Initialize and Test························.PASS
   Ethernet Physical Test·····························PASS
---------------Power-On Self Test Completed---------------------------


Press [Ctrl+B] to enter back door or any key to continue···
```

起動には約60秒を要する。

POST終了時 (最終行を参照) に表示される自動起動メッセージは、起動中に問題が無かったことを示す。 **BootROM Back Door Command Line Interface** (**BootROMバックドア・コマンド・ライン・インターフェイス**) を使用して特殊手順を実行できる。 **BootROM Back Door CLI**に入るには、Ctrl+Bを自動起動メッセージ表示から2秒以内に押す。 Ctrl+Bを押してもシステム起動が中断されない場合、RAMにロード中コードを解凍し続ける。 コードはRAMから実行を開始し、番号付システム・ポート・リストとその状態 (アップリンクかダウンリンクか) が表示される。 デバイスの起動が完了すると、システム・プロンプトが表示されるので、ここからデバイスを構成する。 デバイスを構成する前に最新ソフトウェア・バージョンがデバイスにインストールされていることを確認する。 最新バージョンでなければ、最新バージョンをダウンロードしてインストールする。 最新バージョンのダウンロードについて詳細は、"ソフトウェア・ダウンロード"の節を参照のこと。

5.6 ソフトウェア・ダウンロード

5.6.1 BootROMバック・ドアCLIから

Xmodemプロトコルによるソフトウェアのダウンロード(未サポート)

ソフトウェアのダウンロード手順は最新バージョンをダウンロードして破損したファイルを交換したりシステム・ソフトウェア (システムおよび起動イメージ) を更新またはアップグレードする必要があるときに行う。

BootROM CLIからソフトウェアをダウンロードするには:

1. BootROM CLI プロンプトから次のコマンドを入力する: xmodem –rb <filename>
2. ハイパーターミナルを使用するときは、ハイパーターミナルのメニューバーから Transfer をクリックする。
3. Filename フィールドにダウンロードするファイルへのパスを入力する。
4. Protocol フィールドで Xmodem プロトコルが選択されていることを確認する。
5. Send をクリックする。 ソフトウェアがダウンロードされる。

デバイス構成を消去する

1. BootROM CLI プロンプトから次のコマンドを入力する

   delete <configuration filename>

   次のメッセージが表示される:

   Are you sure you want to delete <configuration filename> (y/n)? (<構成ファイル名>を本当に削除するか、の意)

2. Y を押す。次のメッセージが表示される:

   Updating partition table, please wait … Done (パーティション・テーブルの更新中、、、、完了、の意)

   Image file <configuration filename> deleted.

3. デバイスの初期構成手順を繰り返す。

起動イメージのダウンロード(未サポート)

Xmodemプロトコルを使用して新たな起動イメージをロードし、それをフラッシュメモリに書き込むと起動イメージが更新される。 起動イメージはデバイスの電源を投入するとロードされる。 ユーザーは起動イメージ・コピーを制御できない。 Xmodemプロトコルで起動イメージをダウンロードするには:

1. ダウンロードするファイルを PC ホスト (イメージ・ファイル) に保存する。
2. BootROM> dir –l コマンドを入力して現在デバイスで実行されているソフトウェア・バージョンを確認する。以下は表示される情報例である:

```
BootROM > dir -l
type          zip     def   date           version       name
------------------------------------------------------------------------------
loader        none    yes   2008/12/14    0.4           sb11a-l-0.4.1214.bin
bootrom        gzip   yes   2008/12/14    0.4           sb11a-b-0.4.1214.biz
runtime        gzip   yes   2008/12/10    0.5           sb11a-ibp-r-0.5.1210.biz

Total: 3 files.
```

3. **BootROM CLI** プロンプトから次のコマンドを入力する： xmodem –rb <filename>
4. ハイパーターミナルを使用するときは、ハイパーターミナルのメニューバーから **Transfer** をクリックする。
5. **Filename** フィールドにダウンロードするファイルへのパスを入力する。
6. **Protocol** フィールドで Xmodem プロトコルが選択されていることを確認する。
7. **Send** をクリックする。 ソフトウェアがダウンロードされる。
8. リセット・コマンドを入力する。 次のメッセージが表示される：

```
BootROM> reset
Are you sure you want to reset the system (y/n)? y

System Resetting…
```

9. Y を入力する。デバイスが再起動する。

5.6.2　オペレーション･コードCLIによる

TFTP/FTPサーバからのソフトウェアがダウンロード

この節はTFTP/FTPサーバからデバイス･ソフトウェアをダウンロードする手順を説明する。 TFTP/FTPサーバはソフトウェアをダウンロードする前に構成しなければならない。

システム･イメージのダウンロード

デバイスが起動し、システム･イメージが保存されているフラッシュメモリの領域からシステム･イメージを解凍すると実行する。 新たなイメージがダウンロードされると、他のシステム･イメージ･コピーに割当てられた別の領域に保存される。 次回の起動時に、デバイスは別のイメージが選択されなければ現在アクティブなシステム･イメージを解凍して実行する。

TFTP/FTPサーバからシステム･イメージをダウンロードするには：

1. IP アドレスがデバイスの 1 個のポートに構成されており、TFTP/FTP サーバに ping が送られることを確認する。
2. ダウンロードするファイルが TFTP/FTP サーバ （イメージ･ファイル） に保存されることを確認する。
3. **(CB)#show version** コマンドを入力して現在デバイスで実行中のソフトウェア･バージョンを確認する。 以下は表示される情報例である：

```
(CB) #show version
 Serial number            :SQ823LW00114
 Hardware Version         :1.0
 Number of ports          :48
 Label Revision Number    :1
 Part Number              :A3C40096531
 Machine Model            :PY CB Eth Switch/IBP 1Gb 36/12
 Loader version           :0.7
 Operation code version   :0.40
 Boot rom version         :0.9
```

4. **(CB)#whichboot** コマンドを入力して、どのシステム･イメージが現在アクティブであるかを確認する。 以下は表示される情報例である：

```
Boot-System....................... Switch
Next Booting Mode................. Switch

              file name              file type    startup   size (byte)
---------------------------------  -----------------------  -------  --------------
   sb11a-b-0.9.0212.biz      Boot-Rom image    Y          373327
              default.cfg     Config File        Y            19204
sb11a-ibp-r-0.40.0227.biz   Operation Code    Y          8233676
```

© 2010 富士通テクノロジー･ソリューションズ

5. **(CB)#copy tftp://{tftp address}/{file name} image {file name}または copy ftp://{ftp address}/{file name} image {file name}** コマンドを入力して新たなシステム･イメージをデバイスにコピーする。 次のメッセージが表示される：

```
(CB) #copy tftp://192.168.2.1/sb11a-sw-r-0.40.0227.img image sb11a-sw-r-0.04.0227.biz


Mode........................................... TFTP
Set TFTP Server IP............................ 192.168.2.1
TFTP Path...................................... ./
TFTP Filename.................................. sb11a-sw-r-0.40.0227.img
Data Type...................................... Code
Destination Filename........................... sb11a-sw-r-0.04.0227.biz


Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n)
```

6. Y を押す。新たなイメージがダウンロードされると、他のシステム･イメージ･コピーに割当てられた別の領域に保存される。
7. **boot-system** コマンドを入力して次の起動用イメージを選択する。 このコマンドの後、**(CB)#whichboot** コマンドを入力して起動システム･コマンドでパラメータとして示されたコピーが次の起動用に選択されたことを確認する。
8. 再ロードのコマンドを入力する。 次のメッセージが表示される：

```
(CB)# reload
Are you sure you would like to reset the system? (y/n) y
```

9. Y を入力する。デバイスが再起動する。



システムには 2 個の実行時イメージのみ保存できる。

5.7 ソフトウェアの起動モードを切り替える

イーサネット･コネクション･ブレードにはスイッチ機能とIBP機能から成る2種類のファームウェア･バージョンが格納されている。 起動時には1つのモードでのみ実行可能である。 別のモードで実行するには、起動モードを変更してイーサネット･コネクション･ブレードを再起動しなければならない。

ソフトウェア･モードを変更するには：

1. (CB)#boot-system mode コマンドを入力して次の再起動後にデバイスで実行するソフトウェア･バージョンを指定する。
2. 次の起動時ソフトウェア･モードを IBP に変更するには、(CB)#boot-system mode IBP コマンドを使用する。
3. 次の起動時ソフトウェア･モードをスイッチに変更するには、(CB)#boot-system mode switch コマンドを使用する。

この変更はパワー･サイクルまたはソフトウェアの再起動サイクルに反映される。



コネクション･ブレードは対応して保存されたファームウェアのデフォルト起動構成により起動する、たとえば、IBP起動はibp構成により、スイッチ起動はスイッチ構成による。 これら2種類の構成は無関係である。

6 スタック機能を理解する

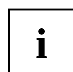
6.1 序文

スタック機能はHiGig/HiGig+ポートのインフィニバンドCX4インターフェイスにより接続されるIBPのグループ・セットである。 すべてのスタック・モジュールを制御するIBPをスタック・マスターと呼ぶ。 他のIBPはスタック・グループのスタック・メンバーに属する。

スタック機能は高密度なポートを提供するが、スタック内すべてのIBPを一点管理できるので管理は容易になる。 スタック内すべてのIBPが1個のIBP製品として動作する。 CLI/Web/SNMP管理には単一IPアドレスを要するが、単一コンソール/telnetｾｯｼｮﾝでスタック全体を管理できる。 PG-SW111 IBPスタックの利点を以下に掲げる。

1. ネットワークで必要とされる IP アドレス数が少なくなる。
2. ネットワークは拡張されてネットワークのより広い帯域を処理できると同時に、小規模グループまたは配線クローゼットの管理が簡素化する
3. 高い可用性機能を提供する。1 ユニットが故障したりケーブルが偶発的に外れても、スタックの他のユニットは稼働を続けるので中断が無い。 (注 1)
4. スタックに参加する新たなユニットはスタックをリセットせずに適切に起動する(注 2) 。
5. スタックから外れるユニットはスタックをリセットせずに適切に取り除ける(注 2) 。
6. マスターの自動選択
7. 構成の自動同期化
8. スタック全体にファームウェア・アップグレードを容易に適用可能

スタック・ソフトウェアは各デバイス・テーブルとレジスターを構成しすべてのスイッチング機能をサポートできる。たとえば、スイッチング、リンクアグリゲーション、ポート監視、スパニング・ツリー・プロトコル、VLAN等がある。スタック全体は単一のIBPとして扱われる。 スタックが正しく機能するために、個々のチップは相互に一貫性を保つようにプログラム化されなければならない。 PG-SW111デバイスがスタックに挿入されたりスタックから抜かれたりすると、全てのチップが動的に構成され、システムが稼働状態を保つことが必要がある。 これはトポロジーを発見し監視するとともにスタックのチップを構成するいくつかのソフトウェア・プロトコルが行う。



1. スタックはフル帯域接続により構成しなければならない (リング・トポロジー)
2. スタックはスタック・マスターを取り除いたり、電源投入状態のスタンドアロン IBP を追加しなければ、メンバーシップ変更の間中断なく稼働状態を保つ。

© 2010 富士通テクノロジー・ソリューションズ

6.2 スタック機能概要

PRIMERGY BX900 GbEコネクション･ブレードの36/8+2スタック(PG-SW111) は次のスタック機能を提供する：

1. リング･トポロジーによるスタックのみ冗長構成をサポートする。 冗長構成機能はリング･トポロジーによるスタックにバックアップ･メンテナンスを保持させなければならない。
2. スタックは最大 8 個のメンバーIBP を含む。
3. スタックは 1 個の IBP として管理され 1 個の IP アドレスのみを持つ。
4. スタックは自動的にマスターIBP をネゴシエートして決める。
5. スタック･マスターが利用できなくなっても、新たなスタック･マスターが残りの IBP から自動的に選ばれる。
6. 自己構成と自己管理
7. IBP は電源投入した IBP を追加する場合を除いて、他の IBP を中断せずにスタックに追加したり取り除ける。
8. LAG はスタック全体のポートで可能であり、1 個の IBP に限定されない。
9. スタック･マスターからは一意の構成入力が行われる。
10. スタック･マスターからは一意のファームウェア･アップグレードの入力が行われる。
11. マスター役は 1 つのユニットからスタック内の他のユニットに移転できる。
12. 状態 LED サポートによりどのデバイスがスタック･マスターかが示される。

© 2010 富士通テクノロジー･ソリューションズ

6.3 スタック·マスターの選定プロセス

PG-SW111のスタック機能は2個の専用12ギガビットHiGig+ポートにより行われる。 このうち1個の専用ポートは内部スタック·リンクと呼ばれる中央部に接続され、別の1個の専用ポートは外部スタック·リンクと呼ばれるフロント·パネルに接続される。 1個のオブジェクトとして容易な管理のために一意の構成入力がサポートされなければならない。 従って、1個のユニットがスタック·マスターとして動作するように選ばれる。 次の節ではスタック·マスター選定プロセスを示す。

スタック·マスター選定の考察は次のようにまとめられる:

1. 同じスタックに他の IBP が無い場合現在スタック·マスターである IBP。
2. 管理者がユーザーの最も高いプライオリティを指定して 1 個の IBP をスタック·マスターに選定できる。
3. 最長時間稼働している IBP を選定する。
4. 最も低い MAC アドレス値がある IBP を選定する。

i

– 再選定プロセスは次のうちいずれかのイベントが生じる場合実施される:
  a) IBP スタックがリセットされた。
  b) IBP マスターがスタックにもはや存在しなくなった。 (スタックから取外された、電源が切られた、まあは故障がある。)
  c) IBP スタック·メンバーシップはシステムまたは IBP スタックに追加の電源が投入された状態のスタンドアロン IBP により増大される。
– IBPプライオリティをユーザーが変更すると、新たなプライオリティはIBPの再起動後または再選定が行われた後にマスター選定プロセスに適用される。
– IBPのプライオリティが無効化されると、スタック·マスターとして二度と選定されない。
– スタックの非マスター·メンバーとして構成されたIBPはスタック·システムにスタック·マスターが存在する場合には、起動時にマスター役を割り当てられない。
– スタックに 1 個以上のスタック·マスターが存在する場合、プライオリティの高い方 (または最長稼働時間、ないし最低MACアドレスがあるもの) がスタック·マスターに選定される。 (これは普通にあるケースではない。 1 個のユニットをスタックに追加する普通の手順は最初からまたは電源投入から 20 秒以内にスタック·ケーブルを接続してから起動する。) 2 個のスタック·マスターがスタックに存在する場合、再選定プロセスが実行されてスタックで 1 個のみのスタック·マスターが選定される。 再選定プロセス後、新たなスタック·マスターは直前のマスターでないこともありえる。 その結果、スタック全体のメンバーが新たなスタック·マスターにより再構成されることとなる。 (その意味は当初の構成が失われることである。) 一方、スタックのトラフィックは中断される。
– 現在のスタック·マスターより高いプライオリティまたは低いMACアドレスのIBPをスタックに接続して起動すると、このIBPが常にスタック·マスターとなる。 推奨される手順は、スタック·マスターにしたいIBPに最も高いプライオリティを割当てればよい。 再選定が行われると、当該IBPがスタックのスタック·マスターとして再選定される。
– スタック·マスターのファームウェア·バージョンと異なるファームウェア·バージョンのIBPはスタックには参加できない。

© 2010 富士通テクノロジー·ソリューションズ

6.4　　ファームウェアのアップグレードと配布プロセス

PG-SW111はファームウェアのアップグレードに2つの方法を提供し、1つはXMODEMにより、他方はTFTP/FTPによる。 ファームウェアのアップグレードはスタック・マスターでのみ実行できる。

アップグレードプロセス

ファームウェアのアップグレードがスタック・マスターで完了すると、スタック・マスターはすべてのスタック・メンバーに向けてダウンロードされたコードを自動配布してスタック内のすべてのメンバーが同じファームウェア・バージョンで実行するようにする。 アップグレードされたコードを実行するためにはスタック・マスターを含むスタック内のすべてのメンバーを再起動することが必要ないし強く推奨される。

配布プロセス

ファームウェアの配布もスタック・マスターからのみ手動で許可される。 スタック・マスターは現在実行中のコードをスタックリンクを通してスタック全体のメンバーまたはスタックの特定メンバーに配布できる。 スタック・マスターはこの機能によりスタック・メンバーのファームウェア・バージョンを同期化できる。 たとえば、異なるファームウェア・バージョンによるIBPがスタックに接続される。 実際には、このIBPはファームウェア・バージョンが異なるためスタックには参加できない。 このIBPをスタックに加える唯一の方法はスタック・マスターからファームウェアを配布することである。 IBPにファームウェアが配布された後、アップグレードされたIBPにユーザーが更新ファームウェアを再ロードすることが必要である。

自動アップグレード・プロセス

ファームウェアの自動アップグレード機能はユーザーが自動アップグレード機能を有効化すればスタック・メンバーに対してサポートされる。 異なるファームウェア・バージョンのIBPがスタックに追加されるにともない、スタック・マスターはフラッシュROMから現在実行中のファームウェアをこのIBPにダウンロードする。 自動アップグレード・プロセスは数秒ないし数分待機してから始まる。 自動アップグレードが完了すると、IBPは(マスターから)再読み込みを求められスタックにフル機能で再度参加するよう要求される。 自動アップグレードには例外がある。 ファームウェア・バージョンの高いIBPがスタックに追加されると、スタック・マスターはたとえ自動アップグレードが有効化されていても自動ではファームウェアアップグレードをこのIBPに対して実行しない。 そのかわりに、スタック・マスターは最小必要なファームウェア・バージョンを示すメッセージを表示する。 これを受けてスタック・マスターとすべてのスタック・メンバーを新たなファームウェアで手動アップグレードをCLIコマンド・セットにより新たなファームウェア・バージョンで実施することを選べる。

スタック・システムデザインにおいては、スタック全体のシステムは新たに追加されたなIBPにより変更や影響を受けることがない。 新たなファームウェア・バージョンのIBPがスタックに追加されると、スタック・システムはアップグレード・プロセスを実行しない。

© 2010 富士通テクノロジー・ソリューションズ

6.5　電源供給

同時に20秒以内に電源オンされたスタック･メンバーはスタック･マスター選定に参加し、スタック･マスターになる可能性がある。 同時に20秒以内に電源オンされたスタック･メンバーが最初の選定に参加しない場合、再選定が行われ、すべてのスタック･メンバーは再選定プロセスに必ず参加させられる。

新たなスタック･マスターは数秒後に利用可能になる。 一方IBPスタックはメモリにある転送テーブルを使用することによりネットワークの停止を最小限にできる。

スタックにあるIBPの電源をオンする前に次のガイドラインを考慮すること。 このガイドラインの目的はスタック･マスターが新たな IBPのスタック･システムへの追加により変更されるのを防止することである。 スタック･マスターが変更されるとトラフィックが中断されて構成も損失する可能性がある。 (スタック･マスターの選定プロセスの節を参照) 初めてインストールする際は、 スタック･システムにおいてスタック･マスターにするIBP に最高のプライオリティを設定することが推奨される。

1. IBP の電源を最初にオンする順序がスタックのマスターになる IBP に影響する可能性がある。
2. 特定の IBP をスタック･マスターにしたい場合、その IBP から電源をオンにすること。 この IBP はスタック･マスターになり、マスター再選定が必要になるまでスタック･マスターにとどまる 約 20 秒後、スタックにある残りの IBP の電源をオンにする。
3. 既存のスタックに追加する IBP はスタック電源の投入後 20 秒以内にスタック･ケーブルによりスタックに接続しなければならない。
4. 電源投入後の IBP を追加する(マージ) とマージする IBP スタックのスタック･マスターにスタック･マスターをその中から再選定させる。 残りの IBP は新たなスタック･マスターにより再構成される。 スタック･マスターが当初からのメンバーでない場合、再構成中にトラフィックは中断される。
5. スタック･マスターを取外すとスタックに新たなスタック･マスターをメンバーの中から再選定させる。 残りの IBP は新たなスタック･マスターにより再構成される。 再構成中にトラフィックは中断される。
6. スタックメンバーを非リング･トポロジーから取外すと、IBP スタックが 2 個またはそれ以上の IBP スタックに分割され(パーティション) 、各パーティションの構成は同じになる。 このためネットワーク内で IP アドレス構成の競合が発生しうる。 IBP スタックを分割されたままにするのであれば、新たに生成された IBP スタックの IP アドレスを変える。 IBP スタックを分割したくない場合：

   a) 新たに生成されたスタックの IBP の電源をオフにする。

   b) スタック･ポートにより当初の IBP スタックにそれらを再度接続する。

   c) 電源を再投入する。

ケース 1: 同じファブリックにある内部スタック･リンクにより2個のIBPをスタック化

たとえば、CB1とCB2をスタックするとする。 CB1をスタック･マスターとする場合、最初にCB1をプラグインする必要がある。その20秒後にCB2をプラグインする。

ファブリック1	SWM1 ◀─▶	SWM2
ファブリック2		
ファブリック3		
ファブリック4		

ケース 2: 異なるファブリックにある外部スタック･リンクにより2個のIBPをスタック化

たとえば、CB1とCB3をスタックするとする。 CB1をスタック･マスターとする場合、最初にCB1をプラグインする必要がある。その20秒後にCB3をプラグインして、20秒以内にCB1とCB3 を外部スタック･ケーブルで接続する。

ファブリック1	▲ SWM1	
ファブリック2	▼ SWM3	
ファブリック3		
ファブリック4		

ケース 3: 内部と外部スタック･リンクによる4個のIBPをスタック化

たとえば、CB1, CB2, CB3,とCB2をスタックするとする。

まずスタック･マスター (CB1)にするSWMをプラグインしてから、20秒後にCB2 をプラグイン(ケース1参照)する必要がある。 次に、CB3をプラグインして、20秒以内にCB1とCB3を外部スタック･ケーブルで接続する。 CB4をプラグインして、最後にCB2とCB4を外部スタック･ケーブルで接続する。

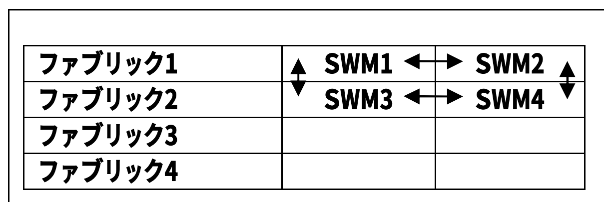
ファブリック1	▲ SWM1 ◀─▶	SWM2 ▲
ファブリック2	▼ SWM3 ◀─▶	SWM4 ▼
ファブリック3		
ファブリック4		



初回のインストール時には、以上の電源供給配慮に従うこと。さもないとどのCBがマスターになるか決まらない (マスター選定プロセスの項目を参照) 。 構成を保存した場合には、同時に電源をオンしてもかまわない。 しかし、外部スタック･ケーブルは電源投入中は常時存在しなければならない。

ケース　4:スタックから故障したスタック･メンバーを交換する

たとえば、CB1、CB2、CB3、及びCB4がスタック･システムを構成し、CB1がスタック･マスター、残りがスタック･メンバー、CB4が故障しているとする。 スタック･システムに影響無くCB4を直接取外せる。 次に、CB4があった場所に新たなCBをプラグインしてCB2とCB4を外部スタック･ケーブルで接続する。 CB4の再起動後、これはスタック･･メンバーとなる。

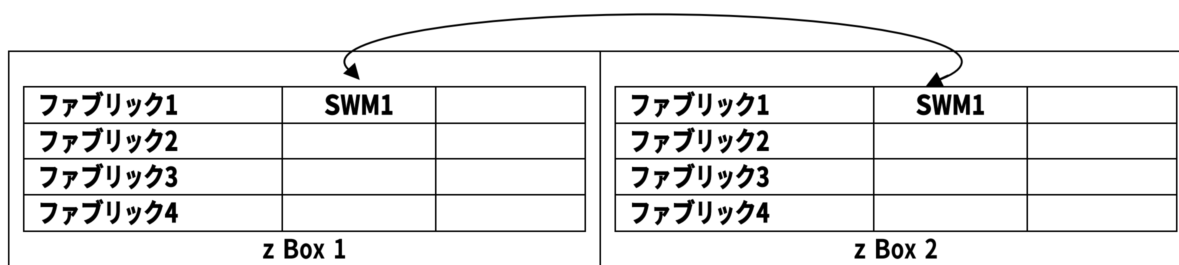


ケース　5: 故障したスタック･マスターをスタックから交換する（ 故障したものがスタック･マスターであれば、残りのスタック･メンバーは新たなスタック･マスターをその中から選定することを意味する)

スタック･マスターであるCB1が故障し、CB1が動作しなくなった後CB2がスタック･マスターになると仮定する。 CB1から外部スタック･ケーブルを外し、ファブリックからCB1を取外す、次にCB1があった場所に新たなCBをプラグインしてから、CB1とCB3を外部スタック･ケーブルで接続する。 CB1の再起動後、これがスタック･メンバーとなる。 CB1をスタック･マスターにする必要があれば、CB2(スタック･マスター)から"switch movemangement <fromunit> <tounit>"コマンドでスタック･マスターをCB2からCB1に移動する。

ケース　6: : 2台のシャーシにまたがりIBP2個をスタック化

zBox 1にある CB1がスタック･マスターであるとすると、zBox 1にCB1を最初にプラグインする必要がある。 次にzBox 2にCB1をプラグインしてから、20秒以内にスタック･ケーブルを接続する。



6.6 スタック·メンバーのプロビジョニング

この機能によりIBPがスタックに参加する前にオフラインで構成できる。 スイッチ番号は1から8の範囲で最も低い未使用番号から割当てられる。スタックをmovemanagementコマンドで構成したり再選定プロセスが実行されない限り、スタック·マスターに最も低い番号が割当てられる。

一意のメンバー番号によりスタック·マスターからスタック·メンバーを生成して、現在スタック·メンバーではない構成済みのIBPに予め機能性を構成できる。 同機種IBPをスタックに追加し、新たなIBPが同じメンバー番号(スイッチ番号) を使用する場合、新たなIBPはスタック·マスターから予め構成されプレ·プロビジョンされた構成を適用される。

© 2010 富士通テクノロジー·ソリューションズ

6.7 名前付けの仕組み

この節はスタック･メンバーの名前付けの仕組みを説明する。 この仕組みを用いて特定のIBPモジュール、IBPモジュールの特定のポートを容易に識別し、操作できる。

MMBがはIBPが読み込む次の情報をISMICを通して与えることが必要である:

1. **ラック名** (読み出しのみ): 今後のために予約されており、空である。
2. **ボックス名** (読み出しのみ): MMB は“Rack1-Encl1-CB1/1/1”の FRU データから連番を取得しこれを“Rack1-Encl1-CB1/1/1”名とする。 (この名前は一意でなければならない。)
3. **ベイ番号** (1-8) (読み出しのみ): MMB により ISMIC を通して静的ベイ番号が割当てられる。
4. **SWM ユーザー定義名** (読み/書き): この欄は IBP のホスト名として使用されるのみであるが、DNS 名としても使用でき、この名前を使用して WebUI から IBP にアクセスできる。

6.7.1 IBP名

IBP名はコネクション･ブレードのユーザー定義名をその名前に使用する。 このデフォルト名は利用可能なインターフェイス(CLI/Web UI) からMMBまたはIBPにより変更でき、ISMICメモリに保存される。 イーサネット･コネクション･ブレードの起動中には常にこの名前をホスト名として読み、DNS名とする。 (注: DNS名はDNSクライアントがサポートされる場合のみ有効である。)

MMBにより指定された名前が無い場合、ホスト名には構成ファイルから保存された名前を用いる。

6.7.2 スタック内の名前付けとアドレス割当て

イーサネット･コネクション･ブレードがシャーシにプラグインされるにともないMMBは必要な名前付け情報を準備しなければならない。 イーサネット･コネクション･ブレードがManagement Blade (MMB)から電源を投入されると、この情報をISMICを通して読み込む。

The MMBはイーサネット･コネクション･ブレードの識別子として<ラック名>-<“Rack1-Encl1-CB1/1/1”名>-CB<ベイ番号> (または<ラック名>が識別されない場合<“Rack1-Encl1-CB1/1/1”名>-CB<ベイ番号>) を使用し、イーサネット･コネクション･ブレードへのISMICのSWMユーザー定義名欄にこの識別子を指定する。 イーサネット･コネクション･ブレードはこの名前"<ラック名>-<“Rack1-Encl1-CB1/1/1”名>-CB<ベイ番号>/<スロット番号>/<ポート>"を使用してイーサネット･コネクション･ブレードのポートを操作する。 <スロット番号>/<ポート>の部分は物理ポートまたは論理ポート (ポートチャネル) の識別に使用される。 たとえば、ボックス1とベイ1の最初のポートチャネルは“Rack1-Encl1-CB1/1/1”として表記される。

7　　E-KEY機能の特長

この節はイーサネット･コネクション･ブレードの全体的メカニズムと要件を含みE-KEY機能の情報を説明する。

MMBはブレード･シャーシ全体の構成を監視できる中央管理部である。 従ってMMBは、イーサネット･コネクション･ブレード、メザニン、及びCPUブレードのE-KEY有効化と無効化機能を制御する中央E-KEYアプリケーションを実行している。 MMBは一方ではIPMIを通してサーバ･ブレード上のBMCに作用してCPUブレードとメザニン･カードのポートを無効化/有効化する。 MMBは他方ではISMICを通してイーサネット･コネクション･ブレードに情報を与え、イーサネット･コネクション･ブレードのダウンリンク･ポートを有効化/無効化する。 イーサネット･コネクション･ブレードへの互換性のあるサーバ･ブレードとメザニンの接続のみコネクション･ブレードの電源オンの際MMBのE-KEYプロセスにより有効化される。 この初期化手順の後、E-KEYプロセスは有効化されたポートをサーバ･ブレード/メザニンまたはコネクション･ブレードのインストール変更に従い最終的に更新する

E-KEY機能は次のようなメカニズムである：

1. イーサネット･コネクション･ブレードの未使用ダウンリンク･ポートを無効化する
2. 非互換のメザニン･カードまたは CPU ブレード･ポートに接続されたイーサネット･コネクション･ブレードのダウンリンク･ポートを無効化する
3. イーサネット･コネクション･ブレードの非互換のダウンリンク･ポートに接続されたメザニン･カードまたは CPU ブレード･チャネルを無効化する
4. 非互換の信号レベルによるハードウェア障害や偽のエラー･メッセージを回避する

イーサネット･コネクション･ブレードの動作：

1. E-KEY 機能はイーサネット･コネクション･ブレードで利用できるすべての構成された機能の可用性と操作性が保持されるように実現される。
2. E-KEY 有効化/無効化機能はイーサネット･コネクション･ブレード(のシャットダウン/非シャットダウン)メザニン･カード(有効化/ 無効化)の既存の利用可能なポート有効化/無効化機能とは無関係である。
3. E-KEY 有効化/無効化機能は標準イーサネット･コネクション･ブレード/メザニン･カードのポート有効化/無効化機能とは無関係でこれらより「低い」”低レベル物理層機能”として実現される。
4. イーサネット･コネクション･ブレードのユーザーインターフェイスすべて (CLI/WebUI)を拡張してダウンリンク･ポート E-KEY 状態を表示できる。

イーサネット･コネクション･ブレードのポートがE-KEY機能により無効化されると、ユーザーによりイーサネット･コネクション･ブレードポートでは有効化できない。しかしユーザーはこれらのポートに通常のスイッチング機能を構成できる。 これらのポートがE-KEY機能により再び有効化されるとユーザーはこれらのポートを有効化も無効化もできる。

ポートがE-KEY機能により無効化されてもユーザーはこのポートに何らかの機能を構成できる。 しかしこのポートはリンクステート機能等ある機能のために内部でファームウェアにより無効化されていることがある。 この場合、当該ポートはE-KEY機能により再び有効化されても無効なままとなる。

© 2010 富士通テクノロジー・ソリューションズ

8　ウェブ･ベース管理インターフェイス

8.1　概　要

BX900イーサネット･コネクション･ブレードにはビルトイン･ブラウザ･ソフトウェア･インターフェイスがあり、Microsoft Internet ExplorerやFirefox等標準ウェブブラウザで遠隔構成と管理ができる。 このソフトウェア･インターフェイスによりイーサネット･コネクション･ブレードのシステム監視と管理もできる。 このイーサネット･コネクション･ブレードをコンソールから始めて構成する際、イーサネット･コネクション･ブレードにIPアドレスとサブネットマスクを割当てなければ成らない。 その後はIBPのIPアドレスをブラウザのアドレス欄に入力すればウェブブラウザから直接イーサネット･コネクション･ブレードのウェブ･ソフトウェア･インターフェイスに直接アクセスできる。 このようにウェブブラウザから、コンソール･ポートに直接接続している感覚で遠隔PCステーションからイーサネット･コネクション･ブレードを管理できる。

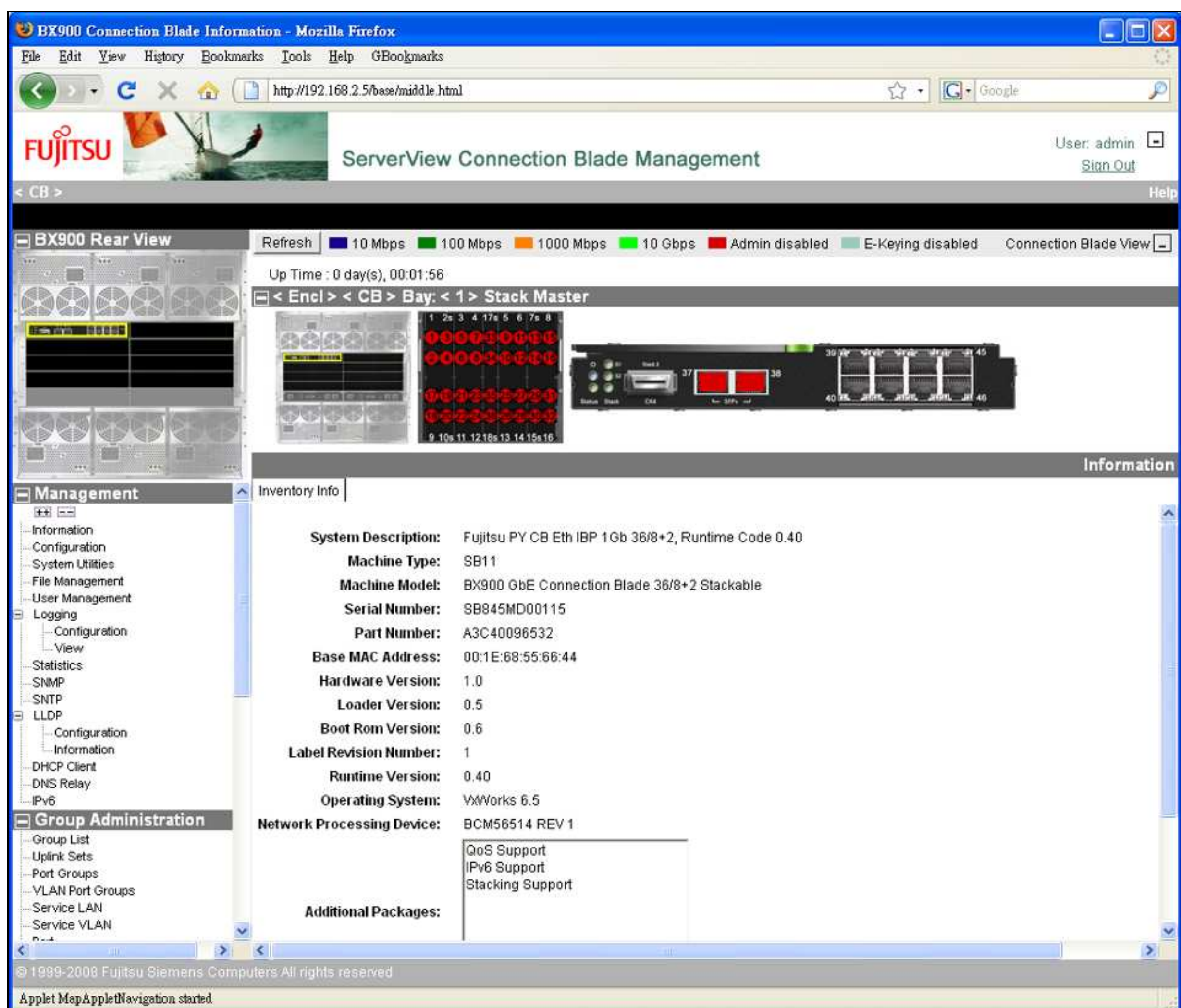


図 ： ウェブ管理インターフェイス

8.1.1 メニュー・オプション

利用できるメニュー・オプション： 管理、スイッチング、グループ管理、セキュリティ、QoS、スタック。

1. **管理メニュー:**

   この節はSNMPとトラップ・マネージャ、Ping、DHCPクライアント、SNTP、及びシステムタイムの構成、Telnetセッションとコンソールのボーレートを含むシステムパラメータの定義、IBPモジュール・ソフトウェアのダウンロード、IBPモジュール、IBP統計、及びレイヤー2MACアドレスのリセットについて説明する。

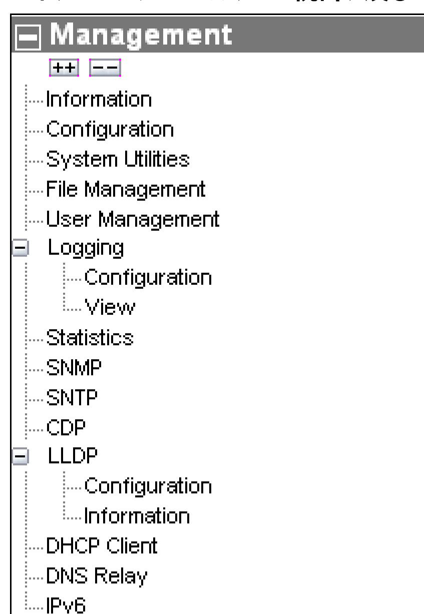


図: 管理メニュー

2. **グループ管理メニュー:**

   この節は、アップリンクセット、ポート・グループ、VLANポート・グループ、サービスLAN、サービスVLAN、ポート、ポート・チャネル、ポート・バックアップの構成方法を説明する。

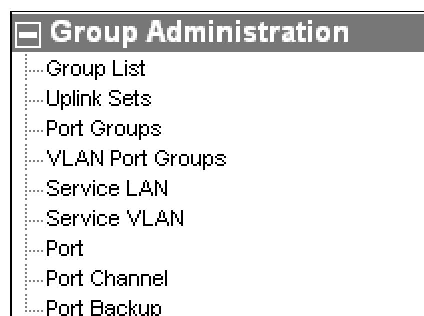


図: グループ管理メニュー

3. **セキュリティ・メニュー:**

この節は、802.1x、 Radius、TACACS、LDAP、 アクセス制御リスト、IPフィルター、https、セキュアシェル等IBPセキュリティの構成方法を説明する。



図: セキュリティ・メニュー

4. **QoS メニュー:**

この節は、DiffServとCoSの構成方法を説明する。



図: QoSメニュー:

5. **スタック・メニュー (スタック可能イーサネット・コネクション・ブレード) :**

この節は、装置のスタックとスタック化装置の実行時コードの更新の構成方法を説明する。

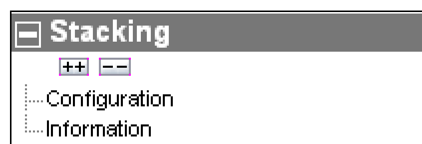


図: スタック・メニュー

8.2 管理メニュー

この節はSNMPとトラップ・マネージャ、Ping、DHCPクライアント、SNTP、及びシステムタイムの構成、Telnetセッションとコンソールのボーレートを含むシステムパラメータの定義、IBPモジュール・ソフトウェアのダウンロード、IBPモジュール、IBP統計、及びレイヤー2MACアドレスのリセットについて説明する。

8.2.1 情報

8.2.1.1 インベントリ情報

Information

Inventory Info

System Description:	FSC PRIMERGY BX900 GbE Connection Blade 36/12, IBP, Runtime Code 0.30
Machine Type:	SB11A
Machine Model:	BX900 GbE Connection Blade 36/12
Serial Number:	SQ903LW00182
Part Number:	A3C40096531
Base MAC Address:	00:23:8B:57:50:9E
Hardware Version:	1.0
Loader Version:	0.6
Boot Rom Version:	0.8
Label Revision Number:	1
Runtime Version:	0.30
Operating System:	VxWorks 6.5
Network Processing Device:	BCM56312 REV 1
Additional Packages:	QoS Support IPv6 Support

Module	Type	Status	Ethernet Compliance Codes	Vendor				
				Name	Part No.	Serial No.	Revision No.	Manufacturing Date

Re

図:インベントリ情報

このパネルは、工場側でIBPの非揮発性メモリに保存された重要な製品データを表示するために使用する。

構成不可能なデータ

System Description/システム内容 - このIBP.の製品名

Machine Type/機種 - このIBP.の機種

Machine Model/モデル - 機種のうちの型式

Serial Number/連番 - IBP.のシリアル番号

Part Number /パーツ番号 - メーカーパーツ番号

Base MAC Address/ベースMACアドレス - MAC.アドレス

Hardware Version/ハードウェア・バージョン - このIBP.のハードウェア・バージョン 最初のバイトはメジャー・バージョンを指し、2番目のバイトはマイナー・バージョンを指す。

Loader Version/ローダー・バージョン - 現在IBPで実行中のローダー・コードのリリース・バージョン・メンテナンス番号 たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。

Boot Rom Version/起動ROMバージョン - 現在IBPで実行中の起動ROMコードのリリース・バージョン・メンテナンス番号 たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。'1.2'.

Label Revision Number/ラベル改訂番号 - ラベルのリビジョンシリアル番号。

Runtime Version/実行時バージョン - 現在IBPで実行中のコードのリリース・バージョン・メンテナンス番号 たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。'1.2'.

Operating System/オペレーティング・システム - このIBPで現在実行中のオペレーティング・システム

Network Processing Device/ネットワーク処理装置 - ネットワーク処理ハードウェアを識別する

Additional Packages/追加パッケージ - 該当する場合には、このIBPにインストール済みのオプション・ソフトウェア・パッケージの一覧表 たとえば、QoS、IPv6やスタック・サポートがある。

Module/モジュール - SFPモジュール名

Type/タイプ - SFPの種類

Status/ｽﾃｰﾀｽ - SFPのステータス

Ethernet Compliance Codesイーサネット準拠コード - トランシーバのコード

Vendor Name/ベンダー名 - SFPトランシーバのベンダー名は、会社の正式名、会社名の一般に通用している略称、会社のSCSI企業コード、あるいは、会社の証券取引所コードのいずれかである。

Vendor Part Number/ベンダー・パーツ番号 - SFPトランシーバのベンダーが割当てたパーツ番号.

Vendor Serial Number/ベンダー連番 - ベンダーが指定するシリアル番号

Vendor Revision Number/ベンダー改訂番号 - ベンダーが割当てたリビジョン番号

Vendor Manufacturing Date/ベンダー製造日 - 製造年月日

コマンドボタン

Refresh/更新 - 頁を最新情報で更新する

© 2010 富士通テクノロジー・ソリューションズ

8.2.2 構成

8.2.2.1 システム内容

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

System Description: FSC PRIMERGY BX900 GbE Connection Blade 36/12, L2+ Switch, Runtime Code 0.14
System Name:
System Location:
System Contact:
In-Band Mgmt IP Address: 0.0.0.0
Out-of-Band Mgmt IP Address: 192.168.2.5
System Object ID: 1.3.6.1.4.1.231
System Up Time: 0 days, 0 hours, 1 mins
Current SNTP Synchronized Time: Not Synchronized

Apply

図: System Description/システム内容

構成可能データ

System Name/システム名 - このIBPを識別するために使用する名前を入力する。 最大31文字までの英数字を使用できる。 工場側デフォルト値は空白である。

System Location/システム所在地 - このIBP.の所在地を入力する。 最大31文字までの英数字を使用できる。工場側デフォルト値は空白である。

System Contact/システム責任者 - このIBP.の責任者名を入力する。 最大31文字までの英数字を使用できる。工場側デフォルト値は空白である。

構成不可能なデータ

System Description/システム内容 - このIBPの製品名

In-Band Mgmt IP Address/インバンド管理IPアドレス - インバンド管理に割当てられた IPアドレス(外部ポートを通してアクセスされる).

Out-of-Band Mgmt IP Address/Out-of-Band管理IPアドレス -Out-of-Band管理に割当てられた IPアドレス(MMBサービス･ポートを通してアクセスされる).

System Object ID/システム･オブジェクト ID - IBPのエンタープライズMIBのベースオブジェクトID

System Up time/システム稼働時間 - 直前のIBP再起動以降経過した時間を日数、時間、分で表記

Current SNTP Synchronized Time/現在のSNTP同期化時間 - UTC単位による現在の同期化SNTP時間 時間が同期化されていない場合、"Not Synchronized"と表示される。

コマンドボタン

Apply - IBP を画面の値で更新する。 IBPにパワー･サイクル後も保持させるには保存を実行する。

8.2.2.2 インバンド管理

インバンド管理はIBPのフロント･パネル･ポートのいずれかを通してIBPとのインバンド接続に使用される論理インターフェイスである。 IBPのインバンド管理に関連付けられた構成パラメータは、トラフィックのスイッチングとルーティングを行うフロント･パネル･ポートの構成には影響しない。

ネットワークからIBPにアクセスするには、IP情報 (IPアドレス、サブネットマスク、デフォルト･ゲートウェイ) で構成を済ませる必要がある。 次の手段のどれでもIP情報の構成を行える:

- BOOTP
- DHCP
- EIA-232ポートを介すする端末インターフェイス (MMBからコンソール･リダイレクトによる)

インバンド接続を確立したら、次のどの手段でもIP情報を変更できる:

- EIA-232ポートを介する端末インターフェイス
- Telnetによる端末インターフェイス
- SNMPによる管理
- ウェブによる管理

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

IP Address:* 0 . 0 . 0 . 0
Subnet Mask:* 0 . 0 . 0 . 0
Default Gateway:* 0 . 0 . 0 . 0
IPv6 Address:
Burned In MAC Address: 00:23:8B:17:7B:85
In-Band Mgmt Protocol: None
DHCP6 Client: Disable
Management VLAN ID:* 1
Web Mode: Enable
Java Mode: Enable
Web Port:* 80

* = mandatory

Apply

図: In-Band Mgmt Config

選択基準

In-Band Mgmt Protocol/インバンド管理プロトコル- IBPの電源投入後の次の動作を指定する: Bootp要求を送る、 DHCP要求を送る、または、何もしない (None). デフォルト設定はNoneである。
この選択はインバンド管理とOOB管理ともに行うことはできない。 OOBインターフェイス構成プロトコルがBootpまたはDHCPに構成されている場合ここでは"None"のみ選択できる。

DHCP6 Client/DHCP6クライアント - DHCP6クライアントが有効化または無効化されるかを選択する。 この選択はインバンド管理とOOB管理ともに行うことはできない。 OOB管理が無効に構成されている場合、ここでは有効化のみ選択できる。

Web Mode/ウェブ･モード - IBPがウェブブラウザからアクセスできるかを指定する。 ウェブモードを有効化すると、ウェブブラウザからIBPを管理できる。 デフォルト設定は有効化されている。

Java Mode/Javaモード

画面右上隅にIBPの画像を表示するJavaアプレットを有効化または無効化する。 このアプレットを実行するとIBPの画像をクリックして、画面左側のナビゲーション・ツリーからではなく構成画面を選択できる。 デフォルト設定は有効化されている。

構成可能データ

IP Address/IPアドレス - インターフェイスのIPアドレス 工場側デフォルト設定値は0.0.0.0である。

Subnet Mask/サブネットマスク - インターフェイスのIPサブネットマスク 工場側デフォルト設定値は0.0.0.0である。

Default Gateway/デフォルト・ゲートウェイ - IPインターフェイスのデフォルト・ゲートウェイ工場側デフォルト設定値は0.0.0.0である。

インバンド管理とOOB管理ともにデフォルト・ゲートウェイを設定することはできない。 OOB管理用ゲートウェイが0.0.0.0に構成されていればゲートウェイを変更できる。

Management VLAN ID/管理VLAN ID -IBPの管理VLAN IDを指定する この値は0～4094の範囲で構成できる。管理VLANはIBPの管理に使用する。 この欄は管理者は構成できるが他のユーザーは読むのみできる。

Web Port/ウェブ・ポート - この選択欄はHTTPポート番号を設定するために使用する。 その値は1～65535の範囲でなければならない。Port80がデフォルト値である。 ウェブページが表示されると現在の構成値が表示される。

構成不可能なデータ

Burned-in MAC Address/焼付けMACアドレス - 焼付けMACアドレスはローカルで管理されるアドレスを構成しないことを選択した場合にインバンド接続に使用される。

IPv6 Address/IPv6アドレス - IPv6アドレスを表示する

コマンドボタン

Apply - IBP を画面の値で更新する。 .パワー・サイクル後、新たな値を保持させるには、保存を実行しなければならない。。

© 2010 富士通テクノロジー・ソリューションズ

8.2.2.3　Out-of-Band管理

Out-of-Band管理インターフェイスはMMBサービス･ポートを通してネットワーク･アクセス接続を提供する。

図:アウトオブバンド管理コンフィグ

このパネルはOOB管理によりネットワークを通してIBPと通信する必要があるパラメータを指定するために用いる。

選択基準

OOBインターフェイス構成プロトコル-　IBPの電源投入後の次の動作を選択する： Bootp要求を送る、DHCP要求を送る、または、何もしない　(None). デフォルト設定はDHCPである。 この選択はインバンド管理とOOB管理ともに行うことはできない。 インバンド管理がBootpまたはDHCPに構成されている場合ここでは”None"のみ選択できる。

DHCP6クライアント - DHCP6クライアントが有効化または無効化されるかを選択する。 この選択はインバンド管理とOOB管理ともに行うことはできない。 インバンド管理が無効に構成されている場合、ここでは有効化のみ選択できる。

構成可能データ

IP Address/IPアドレス - インターフェイスのIPアドレス . 工場側デフォルト設定値は0.0.0.0である。

Subnet Mask/サブネットマスク - インターフェイスのIPサブネットマスク 工場側デフォルト設定値は0.0.0.0である。

Default Gateway/デフォルト･ゲートウェイ - IPインターフェイスのデフォルト･ゲートウェイ 工場側デフォルト設定値は0.0.0.0である。

デフォルトゲートウェイはインバンド管理とOOB管理ともに設定できない。 インバンド管理用ゲートウェイが0.0.0.0に構成されていればゲートウェイを変更できる。

構成不可能なデータ

焼付けMACアドレス - バーインMACアドレスはOOB接続に使用される。

IPv6アドレス - IPv6アドレスを表示する

コマンドボタン

Apply - IBP を画面の値で更新する。 IBPにパワー・サイクル後も保持させるには保存を実行する。

8.2.2.4 Telnetセッション

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

Telnet Session Timeout (minutes) (1 to 160):* 5
Maximum Number of Telnet Sessions: 5
Allow New Telnet Sessions: Yes
Telnet Server Admin Mode: Enable
Password Threshold (0 to 120):* 3

* = mandatory

Apply

図 ：Telnetセッション・コンフィグ

選択基準

Maximum Number of Telnet Sessions/Telnet最大セッション数 - 同時に許可するTelnetセッション数をプルダウン・メニューから選択する 最大セッション数は5であり、これはデフォルト値でもある。

Allow New Telnet Sessions/新たなTelnetセッションを許可する - これをNoに設定すると、新たなTelnetセッションは許可されなくなる。 デフォルト設定は可能 (Yes) である。

Telnet Server Admin Mode/Telnetサーバの管理モード - インバンドTelnetセッションの管理モード この値を無効化に設定するとTelnetポートを遮断する。 管理モードが無効化されていると、すべての既存のTelnet接続が切断される。 デフォルト値は有効である。

構成可能データ

Telnet Session Timeout/Telnetセッション・タイムアウト (分) - Telnetセッションで動作が無い場合セッションがログオフされるまでの分数を指定する。 1～160の範囲で任意の数字を入力できる。デフォルト値は5である。

Password Threshold/パスワード閾値 - ログオン試行の回数限度にコンソール・ポートで到達すると、システム・インターフェイスは次のログオン試行を許可するまでは所定時間応答を止める。 (silent time コマンドでこの間隔を設定する。) Telnetでこの閾値に到達するとTelnetのログオン・インターフェイスは閉じる。

コマンドボタン

Apply - IBP を画面の値で更新する。 IBPにパワー・サイクル後も保持させるには保存を実行する。

© 2010 富士通テクノロジー・ソリューションズ

8.2.2.5 Telnetクライアント･コンフィグ

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

Admin Mode: Enable
Maximum Sessions: 5
Session Timeout(minutes) (1 to 160):* 5
Terminal Length (10 to 100):* 24
* = mandatory

Apply

図 : Telnetクライアント･コンフィグ

選択基準

Admin Mode/管理モード - アウトバウンドTelnetサービスが有効化または無効化されているかを指定する。 デフォルト値は有効化である。

Maximum Sessions/最大セッション数 - 許容最大アウトバウンドTelnetセッション数を指定する。 デフォルト値は5である。値の有効範囲は0から5である。

構成可能データ

Session Timeout/セッション･タイムアウト - アウトバウンドTelnetのログイン試行無しのタイムアウトを指定する。 デフォルト値は5である。値の有効範囲は1から160である。

Terminal Length/端末長さ -コンソールの最大スクロール･ライン数を指定する。

コマンドボタン

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。

© 2010 富士通テクノロジー･ソリューションズ

8.2.2.6　シリアルポート

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

Serial Port Login Timeout (minutes) (0 to 160):* 5
Baud Rate (bps): 115200
Character Size (bits): 8
Flow Control: Disabled
Stop Bits: 1
Parity: None
Password Threshold (0 to 120):* 3
Silent Time (Sec) (0 to 65535):* 0
Terminal Length (10 to 100):* 24

* = mandatory

Apply

図：シリアルポート･コンフィグ

選択基準

ボーレート (bps) - プルダウンメニューからシリアルポート接続のデフォルト速度を選択する。 1200、2400、 4800、 9600、19200、38400、57600、115200ボーから選択できる。 工場側デフォルト設定は9600である。



ボーレートを変更すると、MMBを通すコンソール･リダイレクトは機能しなくなる。

構成可能データ

Serial Port Login Timeout/シリアルポートのログイン･タイムアウト(分) - IBPが接続を終了するまでのシリアルポート接続の動作無し分数を指定する。 0～160の範囲で数字を入力する： デフォルト値は5である。***0を入力するとタイムアウトは無効化される。***

Password Threshold/パスワード閾値 - ログオン試行の回数限度にコンソール･ポートで到達すると、システム･インターフェイスは次のログオン試行を許可するまでは所定時間応答を止める。 (silent time コマンドでこの間隔を設定する。) Telnetでこの閾値に到達するとTelnetのログオン･インターフェイスは閉じる。

Silent Time/静止時間 (秒) - パスワード閾値コマンドにより設定された閾値を失敗したログオン試行回数が超過した後、管理コンソールにアクセス不能になるまでの時間をこのコマンドで設定する。

Terminal Length/端末長さ -コンソールの最大スクロール･ライン数を指定する。

構成不可能なデータ

Character Size (bits)/文字サイズ (ビット) - 一文字のビット数。 この値は常に8である。

Flow Control/フロー制御 - ハードウェア･フロー制御が有効化されるか無効化されるかを指定する。 これは常時無効化されている。

Stop Bits/ストップビット - 一文字毎のストップビット数 これは常時1である。

Parity/パリティー - シリアルポートで使用されるパリティーの方法 これは常時無しである。

コマンドボタン

Apply -IBP を画面の値で更新する。 IBPにパワー・サイクル後も保持させるには保存を実行する。

© 2010 富士通テクノロジー・ソリューションズ

8.2.2.7 HTTP コンフィグ

Configuration

System Description | In-Band Mgmt | Out-of-Band Mgmt | Telnet Session | Telnet Client Config | Serial Port | HTTP Config | DDNS Config

HTTP Session Soft Timeout (Minutes) (0 to 60) :* 15

HTTP Session Hard Timeout (Hours) (0 to 168) :* 24

Maximum Number of HTTP Sessions (0 to 16) :* 16

* = mandatory

Apply

図： HTTP コンフィグ

構成可能データ

HTTP Session Soft Timeout/HTTPセッション･ソフト･タイムアウト - この欄はHTTPセッションの無動作タイムアウトを設定するために使用される。 その値は0～60分の範囲で定める。 0に設定するとタイムアウトは無限大となる。 デフォルト値は15分である。ウェブページが表示されると現在の構成値が表示される。.

HTTP Session Hard Timeout/HTTPセッション･ハード･タイムアウト - この欄はHTTPセッションのハード･タイムアウトを設定するために使用される。 このタイムアウトはセッションの動作レベルには影響されない。 その値は0～168時間の範囲で定める。 0に設定するとタイムアウトは無限大となる。 デフォルト値は24時間である。 ウェブページが表示されると現在の構成値が表示される。.

Maximum Number of HTTP Sessions/最大HTTPセッション数 - この欄はHTTPセッションの最大許容数を設定するために使用される。 その値は0～16回の範囲で定める。 デフォルト値は16時間である。ウェブページが表示されると現在の構成値が表示される。

コマンドボタン

Apply - 更新された画面をIBPに送る。

パワー･サイクル後、新たな値を保持させるには、保存を実行しなければならない。

8.2.2.8　　DDNSコンフィグ

図 ：DDNSコンフィグ

選択基準

DDNSホスト - データが表示されるまたは構成される DDNSホストを選択する。 項目を追加するが選択されると、新たなDDNSホストを構成できる。

サーバ･タイプ - DDNSサーバのサーバ･タイプを選択する。 次のどれでも選べる：

- EASYDNS
- DYNDNS
- DHS
- ODS
- DYNS
- ZONEEDIT
- TZO

構成可能データ

Host Name/ホスト名 - DDNSサーバのホスト名

User Name/ユーザー名 - DDNSサーバのユーザー名

Password/パスワード - アカウント用の新規オプションまたは変更パスワードで、タイプした文字列は表示されず、アスタリスク(*)のみ見える。 パスワードは最大長32文字で大文字と小文字は区別される。

IP Address/IPアドレス - IPアドレスはユーザーが設定する"ホスト名"にマップされる。

Server IP/サーバIP -このオプションを選択するとIPアドレスはインバンド管理IPアドレスに設定される。

コマンドボタン

Apply - IBPに更新された画面を設定し、IBPに変更を有効化するが、変更は保存を実行しないとパワー･サイクル後保持されない。

Remove/削除 - 選択されたDDNS構成を削除する

8.2.3 システム・ユーティリティー

8.2.3.1 すべての変更を保存する



図 ： すべての変更を保存する

コマンドボタン

Save/保存 - このボタンをクリックしてオンすればシステムが再起動しても構成の変更は保存される。 直前の保存またはシステム再起動以降に送信されたすべての変更はIBPに保持される。

8.2.3.2 システムのリセット



図 ： システムのリセット

コマンドボタン

Reset/リセット - IBPを再起動するにはこのボタンを選択する．直前に保存を実行して以降行った構成変更は全て消去される。 このボタンを選択した後、確認画面が表示される。

8.2.3.3　　コンフィグをデフォルトに設定する

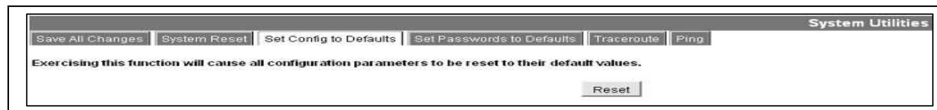


図 :コンフィグをデフォルトに設定する

コマンドボタン

Reset/リセット - すべての構成パラメータを工場側デフォルト設定値にリセットするためにはこのボタンを選択する。

これまでに行ったすべての変更は、保存を実行したとしても消去される。 このボタンを選択した後、確認画面が表示される。 .

8.2.3.4　　パスワードをデフォルトに設定する

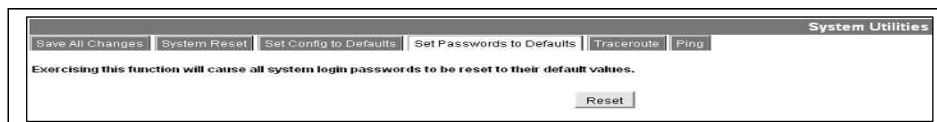


図 :パスワードをデフォルトに設定する

コマンドボタン

Reset/リセット Resetボタンをクリックするとすべてのシステム･ログイン用パスワードはデフォルト値にリセットされる。

パワー･サイクル後、新たな値を保持させるには、保存を実行しなければならない。

8.2.3.5 Traceroute

IBPに指定したIPアドレスへTraceRouteの要求を送信するように指示するためにはこの画面を使用する。 この画面を使用して遠隔ターゲットにパケットが届くまでの経路を見つけることができる。 Applyボタンをクリックすると、IBPはtracerouteコマンドを送り、その結果は構成可能データの下に表示される。 tracerouteコマンドに応答がると、次の内容が表示される：

1 x.y.z.w   1 ms 2 ms 3 ms

2 0.0.0.0   0 ms 0 ms 0 ms

3 0.0.0.0   0 ms 0 ms 0 ms

System Utilities

Save All Changes | System Reset | Set Config to Defaults | Set Passwords to Defaults | Traceroute | Ping

IPv4 Address

Probes Per Hop (1 to 10):* 3

MaxTTL (1 to 255):* 20

InitTTL (1 to 255):* 1

Interval(secs) (1 to 60):* 3

TraceRoute:

* = mandatory

Apply

図 ：Traceroute

構成可能データ

IP Address/Host Name/IPv6 Address | IPアドレス/ホスト名/IPv6アドレス - IBPに経路を発見させたいステーションのアドレスを入力する 初期値は空白である。入力するアドレスはパワー・サイクル後、保持されない。

Probes Per Hop/ホップ毎のプローブ - ホップ毎にプローブ数を入力する 初期値はデフォルトである。 入力するホップ毎のプローブはパワー・サイクル後、保持されない。

MaxTTL - ターゲットに対する最長TTLを入力する 初期値はデフォルト値である。 入力するMaxTTLはパワー・サイクル後、保持されない。

InitTTL - 使用する初期TTL値を入力する 初期値はデフォルト値である。 入力するInitTTL はパワー・サイクル後、保持されない。

Interval/間隔 - プローブ間の時間を秒で入力する 初期値はデフォルト値である。 入力する間隔秒数はパワー・サイクル後、保持されない。

コマンドボタン

Apply - traceroute.コマンドを実行する

8.2.3.6 Ping

IBPに指定したIPアドレスへPingの要求を送信するように指示するためにはこの画面を使用する。 IBPが特定のIPステーションと通信できるかを調べるために使用できる。 Applyボタンをクリックすると、IBPは3つのpingコマンドを送り、その結果はconfigurable dataの下に表示される。 pingコマンドに応答が無いと、次の内容が表示される：

No Reply Received from IP xxx.xxx.xxx.xxx (IP xxx.xxx.xxx.xxxから応答無し)

それ以外の場合には次が表示される：

Reply received from IP xxx.xxx.xxx.xxx (IP xxx.xxx.xxx.xxxから応答を受信した) : (send count = 3, receive count = n) (送信数=3、受信数=n)

図 : Ping

選択基準

Address Type/アドレス・タイプ - Select the address type for IPv4アドレス、ホスト名またはIPv6アドレスのアドレス・タイプを選択する。

構成可能データ

次のオプションはユーザーが選択するアドレスに従う：

- IPv4:

IP Address/IPアドレス - IBPがpingを送るべきターゲット・ステーションの IPアドレスを入力する 初期値は空白である。入力するIPアドレスはパワー・サイクル後、保持されない。

- ホスト名：

Host Name/ホスト名 - IBPがpingを送るべきターゲット・ステーションの ホスト名を入力する

- IPv6:

Ping - PingのターゲットであるグローバルIPv6アドレスまたはリンク・ローカル・アドレスを選択する

次のオプションはユーザーが選択するPingの種類に従う：

- グローバル：

  IPv6 Address/IPv6アドレス - IBPがpingを送るべきターゲット・ステーションの IPv6アドレスを入力する

- リンク・ローカル：

  Management Type/管理タイプ - インバンドまたはout-of-band管理を選択する

  Link Local Address/リンク・ローカル・アドレス - IBPがpingを送るべきターゲット・ステーションのリンク・ローカル・アドレスを入力する 初期値は空白である。

  Datagram Size/データグラムのサイズ - データグラムのサイズを入力する 有効な範囲は48から2048までです。

構成不可能なデータ

Ping Output/Pingの出力 - IBPから受信された応答結果

コマンドボタン

Apply - Pingを初期化する

© 2010 富士通テクノロジー・ソリューションズ

8.2.4　ファイル管理

8.2.4.1　IBPへダウンロードする

ファイルをIBPへダウンロードするにはこのメニューを使用する。

File Management

Download To IBP | Upload From IBP | Start-Up File | Remove File | Copy File

File Type: Code
Protocol Mode: TFTP
FTP/TFTP Server IP Address:* 0 . 0 . 0 . 0
FTP/TFTP File Path (Source):*
FTP/TFTP File Name (Source):*
FTP/TFTP File Name (Target):*
Start File Transfer
* = mandatory
Apply

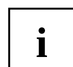
図 : ファイルをIBPへダウンロードする

選択基準

File Type/ファイル･タイプ - ダウンロードするファイルのタイプを指定する: (ファイル･タイプのデフォルト値はコード)

- **Script/スクリプト** -IBPのスクリプト･ファイルを更新する際に構成スクリプトを指定する
- **CLI Banner/CLIバナー** - CLIインターフェイスのバナー
- **Code/コード** - 動作フラッシュメモリをアップグレードする際のコードを指定する
- **Configuration/構成** - IBPの構成を更新する際に構成を指定する ファイルにエラーがあると更新は中止される。
- **SSH-1 RSA Key File/SSH-1 RSAキーファイル**- SSH-1 リベスト-シャミア-エーデルマン (RSA) キーファイル
- **SSH-2 RSA Key PEM File/SSH-2 RSAキーPEMファイル**- SSH-2 リベスト-シャミア-エーデルマン (RSA) キーファイル(PEMエンコード)
- **SSH-2 DSA Key PEM File/SSH-2 DSAキーPEMファイル**- SSH-2 デジタル署名アルゴリズム (DSA) キーファイル(PEMエンコード)
- **SSL Trusted Root Certificate PEM File/SSL 信頼されたルート証明書 PEMファイル** - SSL 信頼されたルート証明書ファイル(PEMエンコード)
- **SSL Server Certificate PEM File/SSL サーバ証明書 PEMファイル** - SSL サーバ証明書ファイル(PEMエンコード)
- **SSL DH Weak Encryption Parameter PEM File/SSL DH 脆弱暗号化パラメータ PEMファイル**- SSL ディフェーヘルマン脆弱暗号化パラメータ･ファイル (PEM Encoded)
- **SSL DH Strong Encryption Parameter PEM File/SSL DH 強化暗号化パラメータ PEMファイル**- SSL ディフェーヘルマン強化暗号化パラメータ･ファイル (PEM Encoded)

•



SSHキーファイルをダウンロードするにはSSHは管理者により無効化されなければならず、アクティブなSSHセッションがあってはならない。

Protocol Mode/プロトコル・モード - ダウンロード・モードに使用するプロトコルを指定する。 FTPかTFTPから選択できる。

構成可能データ

FTP/TFTP Server IP Address/FTP/TFTP サーバIP アドレス - FTP/TFTP サーバのIP アドレスを入力する。　工場側デフォルトは0.0.0.0である。

FTP/TFTP File Path (Source)/FTP/TFTPファイル・パス(ソース) - 選択されたファイルをアップロードする。 FTP/TFTP サーバ上のパスを指定する 最大96文字まで入力できる(区切りスラッシュを含む) 。 工場側デフォルト値は空白である。 .

TP/TFTP File Name (Source)/FTP/TFTPファイル名(ソース) - 選択されたファイルをダウンロードする。 FTP/TFTP サーバ上の名前を入力する 最大32文字まで入力できる。　工場側デフォルト値は空白である。 . .

FTP/TFTP File Name (Target)/FTP/TFTPファイル名(ターゲット) - 保存するファイルのIBP上の名前を入力する。　最大30文字まで入力できる 工場側デフォルト値は空白である。 .

Start File Transfer/ファイル転送の開始 - ダウンロードを開始するにはこのチェックボックスをオンしてからApplyボタンを選択する。

構成不可能なデータ

テーブルの最終行にファイル転送状態を示す。 画面はファイル転送が完了するまで自動的に更新する。

コマンドボタン

Apply -更新された画面をIBPに送りファイルのダウンロードを実行する。

8.2.4.2 IBPからアップロードする

コード、構成またはログファイルをIBPからアップロードするためにはこのメニューを使用する。

File Management

Download To IBP	Upload From IBP	Start-Up File	Remove File	Copy File

File Type: CLI Banner
Protocol Mode: TFTP
FTP/TFTP Server IP Address:* 0 . 0 . 0 . 0
FTP/TFTP File Path (Target):*
FTP/TFTP File Name (Target):*
Start File Transfer

* = mandatory

Apply

図：ファイルをIBPからアップロードする

選択基準

ファイル・タイプ - アップロードするファイルのタイプを指定する 利用可能なオプションはスクリプト、コード、CLIバナー、構成、エラー・ログ、バッファー・ログ、トラップ・ログである。 工場側デフォルトはコードである。

プロトコル・モード - アップロード・モードに使用するプロトコルを指定する FTPかTFTPから選択できる。

構成可能データ

FTP/TFTP Server IP Address / FTP/TFTP サーバIP アドレス - Enter the IP address of the FTP/TFTP server. The factory default is 0.0.0.0.

FTP/TFTP File Path (Target)/FTP/TFTPファイル・パス(ターゲット) - アップロードするファイルの保存先。FTP/TFTP サーバ上のパスを指定する 最大96文字まで入力できる(区切りスラッシュを含む)。 工場側デフォルト値は空白である。 .

FTP/TFTP File Name (Target) /FTP/TFTPファイル名(ターゲット) - アップロードするファイルに付けたい名前を入力する。 最大32文字まで入力できる 工場側デフォルト値は空白である。 .

FTP/TFTP File Name (Source)・FTP/TFTPファイル名 (ソース) - IBPからアップロードするファイルを指定する。

Start File Transfer/ファイル転送の開始 - アップロードを開始するにはこのチェックボックスをオンしてからApplyボタンを選択する。

構成不可能なデータ

テーブルの最終行にファイル転送進捗を示す。 画面はファイル転送が完了するまで自動的に更新する。 .

コマンドボタン

Apply - 更新された画面をIBPに送りファイルのダウンロードを実行する。.

8.2.4.3　起動ファイル

システムの起動に使用されるファイルを指定する。

File Management

Download To Switch | Upload From Switch | Start-Up File | Remove File | Copy File

Current Configuration File: factory_default
Current Runtime File: img61
Configuration File: factory_default
Runtime File: img61

Apply

図 ： 起動ファイル･コンフィグ

選択基準

Configuration File/構成ファイル -構成ファイルの

Runtime File/実行時ファイル - 実行時動作コード.

構成不可能なデータ

Current Configuration File/現在の構成ファイル -現在の構成ファイル

Current Runtime File/現在の実行時ファイル - 現在の実行時動作コード.

コマンドボタン

Apply - 更新された画面をIBPに送り、ファイル起動を指定する。

© 2010 富士通テクノロジー･ソリューションズ

8.2.4.4　　ファイルを削除する

フラッシュメモリ内のファイルを削除する。 システム起動にファイルが使用された場合、このファイルは削除できない。



図 ： ファイルを削除する

選択基準

Configuration File/構成ファイル -構成ファイルの

Runtime File/実行時ファイル - 実行時動作コード.

Script File/スクリプト・ファイル - 構成スクリプト・ファイル

コマンドボタン

Remove/削除 - 更新された画面をIBPに送りファイルの削除を実行する。

8.2.4.5　ファイルをコピーする

IBP上の実行構成ファイルから起動構成ファイルをコピーするにはこのメニューを使用する。

図　: ファイルをコピーする

構成可能データ

File Name/ファイル名 - コピーするファイルに付けたい名前を入力する 最大30文字まで入力できる。 工場側デフォルト値は空白である。 .

構成不可能なデータ

テーブルの最終行にファイル・コピーの進捗を示す。 画面はファイルのコピーが完了するまで自動的に更新する。

コマンドボタン

Copy to File/ファイルへコピーする - 更新された画面をIBPに送りファイルのコピーを実行する。

8.2.5 ユーザー管理

8.2.5.1 ユーザー･アカウント

デフォルトでは2人のユーザー･アカウントがある：

- 管理者、読み･書き特権付き
- ゲスト、読みのみ特権付き

デフォルトでは管理者のパスワードは“admin”でゲストは空白である。 名前は大文字と小文字の区別をしない。

読み･書き特権付きユーザー･アカウントに(すなわち、管理者として)ログオンすると、このユーザー･アカウントを用いてパスワードを割当て、デフォルト･アカウントのセキュリティ･パラメータを設定し、最大6個までのアカウント(管理者以外)を追加、削除できる。

User Management

User Accounts | Authentication List Config | Authentication List Summary | User Login | Login Session

User: admin
User Name:* admin
Password: •••••
Confirm Password: •••••
Access Mode: Read/Write
SNMP v3 User Configuration
SNMP v3 Access Mode: Read/Write
Authentication Protocol: None
Encryption Protocol: None
Encryption Key: Apply
* = mandatory
Apply

図 ： ユーザー･アカウント･コンフィグ

選択基準

User/ユーザー - 既存アカウントを再構成する、または新たなアカウントを生成するにはこの画面を使用できる。 既存アカウントから1個を選択するにはこのプルダウンメニューを使用し、または'Create'を選択して新たなアカウントを追加するが、最大5個の'Readのみ'のアカウントに到達していないことが条件である。

Authentication Protocol/認証プロトコル - 選択されたユーザー･アカウントのSNMPv3 認証プロトコル設定を指定する。 有効な認証プロトコルは無し、MD5またはSHAである。 無しを選択すると、SNMPブラウザからSNMPデータにアクセスできなくなる。 MD5またはSHAを選択すると、ログイン･パスワードがSNMPv3認証パスワードとして使用されるので、パスワードは指定しなければならない。長さは8文字とする。

Encryption Protocol/暗号化プロトコル - 選択されたユーザー･アカウントのSNMPv3暗号化プロトコル設定を指定する。 有効な暗号化プロトコルは無しまたはDESである。 DESプロトコルを選択すると、暗号化キーの欄にキーを入力しなければならない。 プロトコル無しを指定した場合、暗号化キーは無視される。

構成可能データ

User Name/ユーザー名 - 新アカウントに付けたい名前を入力する （新アカウントを生成するときのみこの欄にデータを入力できる。）。 ユーザー名の長さは8文字まで、大文字と小文字の区別は無い。 有効な文字はすべての英数字に加え、ダッシュ ('-') とアンダースコア ('_')を使用できる。 "default"というユーザー名は無効である。

Password/パスワード - アカウントにオプションの新規または変更パスワードを入力する。タイプした文字列は表示されず、アスタリスク(*)のみ見える。 パスワードは8文字までの英数字で大文字と小文字は区別される。

Confirm Password/パスワードを確認する - パスワードを再入力して、正しく入力したことを確認する。この欄は文字は表示せずアスタリスク(*)を示す。

Encryption Key/暗号化キー - 暗号化プロトコル欄でDESを選択した場合、SNMPv3暗号化キーをここに入力する。 それ以外の場合この欄は無視される。 有効なキーは8から64文字までである。 暗号化プロトコルと暗号化キーを変更するためにはApplyチェックボックスをオンにする。

構成不可能なデータ

Access Mode/アクセス･モード - ユーザーのアクセス･モードを示す。 管理者アカウントは常時'Read･Write'アクセスであり、その他すべてのアカウントは'Readのみ'の特権である。

SNMP v3 Access Mode/SNMP v3 アクセス･モード - ユーザー･アカウントのSNMPv3アクセス特権を示す。 管理者アカウントは常時'Read･Write'アクセスであり、その他すべてのアカウントは'Readのみ'の特権である。

コマンドボタン

Apply - IBP を画面の値で更新する。IBPにパワー･サイクル後、値を保持させるには、保存を実行しなければならない。.

Delete/削除 - 現在選択されているユーザー･アカウントを削除する。 IBPにパワー･サイクル後、保持させるには、保存を実行しなければならない。. このボタンは'Readのみ'アクセス特権のユーザー･アカウントを選択した場合のみ見える。 'Read･Write'アクセス特権のあるユーザーを削除できない。

© 2010 富士通テクノロジー･ソリューションズ

8.2.5.2　認証リスト･コンフィグ

この画面はログイン･リストを構成するために使用する。 ログイン･リストはリストに関連付けられたユーザーのIBPないしポートへのアクセスを認証するために使用する認証方法を指定する。 初期設定ユーザーである管理者とゲストは削除できないデフォルト･リスト名の初期構成リストに割当てられている。 すべての新たに生成されたユーザーも異なるリストに割当てるまではデフォルト･リストに割当てられる。

User Management
User Accounts | Authentication List Config | Authentication List Summary | User Login | Login Session
Authentication List: Create
Authentication List Name:*
* = mandatory
Apply

図 ： 認証リスト･コンフィグ

選択基準

Authentication List/認証リスト - 構成する認証ログイン･リストを選択する。 'Create/生成する'を選択して新たなログイン･リストを定義する。 新たなログイン･リストを生成する際、'ローカル'は初期認証方法として設定される。

Method 1/方法1 - 選択された認証ログイン･リストにまず表示される方法を選択するためにこのドロップダウンメニューを使用する。 'ローカル'等最初の方法としてタイムアウトしない方法を選ぶと、たとえ1個以上の方法を指定しても他の方法は試行されない。 このパラメータはまず新たなログイン･リストを生成すると表示される。 オプション：

- **Local/ローカル** - ローカルに保存されたユーザー名とパスワードが認証に使用される。
- **Radius** - ユーザー名とパスワードはローカルではなくRADIUSサーバにより認証される。
- **TACACS+** -ユーザー名とパスワードはTACACS+サーバにより認証される。
- **LDAP**-ユーザー名とパスワードはLDAPサーバにより認証される。
- **Reject/拒否**- ユーザーは認証を常に拒否される。
- **Undefined/未定義** - 認証方法は未定である(この選択肢は最初の方法として割当てられない)。

Method 2 /方法2 -選択された認証ログイン･リストに2番目に表示される方法ーこれを選択するためにこのドロップダウンメニューを使用する。 これは最初の方法がタイムアウトした場合に使用される方法である。 2番目の方法としてタイムアウトしない方法を選択すると3番目の方法は試行されない。このパラメータはまず新たなログイン･リストを生成すると表示される。

Method 3 /方法3 -選択された認証ログイン･リストに3番目に表示される方法ーこれを選択するためにこのドロップダウンメニューを使用する。 このパラメータはまず新たなログイン･リストを生成すると表示される。

構成可能データ

Authentication List Name/認証リスト名 - 新たなログイン･リストを生成する場合、割当てる名前を入力する。 最大15文字の英数字であり、大文字と小文字を区別しないものとする。

コマンドボタン

Apply - 更新された画面をIBPに送りIBPで変更を有効化する。 当該変更は保存を実行しないとパワー･サイクル後、保持されない。

Delete/削除 - 選択された認証リストを構成から削除する。 システム･ログインまたはIEEE 802.1xポート･アクセス制御で任意のユーザーに(デフォルト･ユーザーを含む)選択されたログイン･リストが割当てられる

と削除は失敗する。 このボタンは読み･書きアクセス特権がある場合のみ使用できる。当該変更は保存を実行しないとパワー･サイクル後、保持されない。

8.2.5.3　　認証リスト･サマリ

User Management

User Accounts | Authentication List Config | Authentication List Summary | User Login | Login Session

Authentication List	Method List	Login Users	802.1x Port Security Users
defaultList	local	admin guest default	admin guest default

Refresh

図 ： 認証リスト･サマリ

構成不可能なデータ

Authentication List/認証リスト -この行に一覧表示された認証ログイン･リストを識別する。

Method List/方法リスト - このログイン･リストに構成された方法の整理されたリスト。

Login Users/ログイン･ユーザー - ユーザー･ログイン構成画面でこのログイン･リストに割当てたユーザー。 このリストはシステム･ログイン･アクセスでユーザーを認証するために使用される。

802.1x Port Security Users/802.1xポート･セキュリティ･ユーザーポート･アクセス制御ユーザー･ログイン構成画面でこのログイン･リストに割当てるユーザーである。このリストはIEEE 802.1xプロトコルによりポート･アクセスを認証するために使用される。

コマンドボタン

更新 - ページ情報を更新する。

8.2.5.4　　ユーザー･ログイン

構成された各ユーザーはIBPまたはIBPのポートにアクセスを試みる際ユーザーを認証する方法を指定するログイン･リストに割当てられる。 ユーザー･アカウント画面で新たなユーザー･アカウントを生成した後、そのユーザーをこの画面からIBPのログイン･リストに、さらに必要であれば、ポート･アクセス制御ユーザー･ログイン構成画面で当該ポートのログイン･リストに割当てる必要がある。 当該ユーザーに新たなログイン･リストを生成する必要があれば、認証リスト構成頁で行う。

初期設定ユーザーである管理者とゲストは削除できないデフォルト･リスト名の初期構成リストに割当てられている。 すべての新たに生成されたユーザーも異なるリストに割当てるまではデフォルト･リストに割当てられる。

IBPにアカウントが構成されていないユーザーは'デフォルト'ないし'未構成'ユーザーとよばれる。 RADIUSサーバを通して認証を指定するログイン･リストに'未構成ユーザー'を割当てる場合、各IBPにすべてのユーザーのアカウントを生成する必要はない。 しかしデフォルトでは'未構成ユーザー'は、デフォルトではローカル認証を使用する'デフォルト･リスト'に割当てられる。

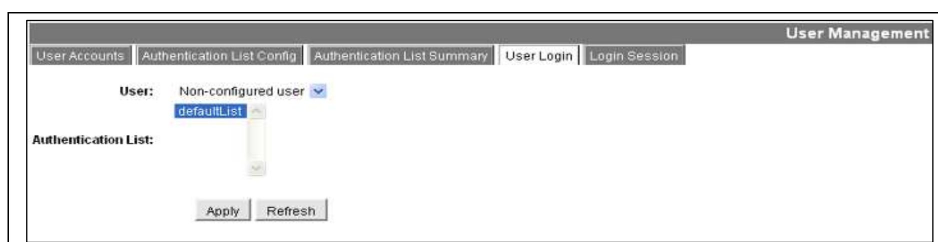


図　:ユーザー･アカウント･コンフィグ

選択基準

User/ユーザー - ログイン･リストに割当てるユーザーを選択する。 管理者は常にデフォルト･リストと関連付けること。 これで管理者は常にローカルで認証されIBP構成から完全に遮断されることがなくなる。 遠隔認証を要求するログイン･リストにユーザーを割当てると、そのユーザーは認証が完了するまではすべてのCLI、ウェブ、TelnetセッションからIBPにアクセスできない。 RADIUS構成ヘルプに最大遅延時間について説明されている。

構成可能データ

Authentication List/認証リスト - システム･ログインでユーザーを割当てる認証ログイン･リストを選択する。

コマンドボタン

Apply -更新された画面をIBPに送りIBPで変更を有効化する。 当該変更は保存を実行しないとパワー･サイクル後、保持されない。.
更新 - ページ情報を更新する。

8.2.5.5　ログイン･セッション

この頁には、ユーザー名、接続元、アイドル･タイム、セッション･タイム、セッション･タイプからなるログイン･セッション情報が表示される。

User Management

User Accounts | Authentication List Config | Authentication List Summary | User Login | Login Session

ID	User Name	Connection From	Idle Time	Session Time	Session Type
00	admin	EIA-232	00:04:09	00:04:20	Serial Port
11	admin	192.168.2.188	00:00:00	00:03:57	HTTP

Refresh

図 : ログインセッション

構成不可能なデータ

- **ID** -この行のIDを指す。
- **User Name/ユーザー名** - セッションを確立したユーザーの名前を示す。
- **Connection From/接続元** - ユーザーがどのマシンから接続しているかを示す。
- **Idle Time/アイドル･タイム** - アイドル･セッション･タイムを示す。
- **Session Time/セッション･タイム** - 合計セッション･タイムを示す。
- **Session Type/セッション･タイプ** - セッション･タイプを示す。: telnet、シリアルポート、SSH または HTTP.

コマンドボタン

- **更新** - ページ情報を更新する。

© 2010 富士通テクノロジー･ソリューションズ

8.2.6 ロギング

8.2.6.1 バッファー·ログを構成する

このログはメッセージの内容と重大度に基づいてメモリにメッセージを保存する。 スタック可能システム上ではこのログはスタック·プラットフォームの最上部にのみ存在する。 スタックの他のプラットフォームはメッセージをスタック·ログの最上部に転送する。



図 :バッファー·ログ·コンフィグ

構成可能データ

Admin Status/管理ステータス - "無効化"されているログはメッセージを記録しない。 "有効化"されているログがメッセージを記録する。 ロギングの有効化と無効化はプルダウン入力欄の該当行を選択する。

Behavior/動作 ログ容量が最大になったときの動作を示す。 ログ容量が最大になると上書きするかしない。

コマンドボタン

Apply - IBP を入力値で更新する。

8.2.6.2　　コマンド･ロガーを構成する

図 : コマンド･ロガー･コンフィグ

選択基準

Admin Mode/管理モード - CLIコマンド･ロギングの有効化/無効化操作はプルダウンの該当欄を選択して、Applyをクリックする。

コマンドボタン

Apply - IBP を入力値で更新する。

8.2.6.3　　コンソール･ログを構成する

これはホストに接続されたどのシリアル機器にもメッセージのロギングを可能にする。

図: コンソール･ログ･コンフィグ

選択基準

Admin Status/管理ステータス - "無効化"されているログはメッセージを記録しない。 "有効化"されているログがメッセージを記録する。 ロギングの有効化と無効化はプルダウン入力欄の該当行を選択する。

Severity Filter/重大度フィルター -ログは構成された重大度閾値に等しいまたはそれを超えるメッセージを記録する。 重大度オプションはプルダウン入力欄の該当行を選択して選択する。 これらの重大度レベルを次に列挙した：

- **Emergency/緊急 (0): システムは使用不可**
- **Alert/アラート (1): 直ちにアクションを要する**
- **Critical/致命的 (2): 致命的な状況**
- **Error/エラー (3): エラー状況**
- **Warning/警告 (4): 警戒を要する状況**
- **Notice/注意(5): 通常ではあるが重要な状況**
- **Informational/情報提供(6): 情報提供のみのメッセージ**
- **Debug/デバッグ(7): デバッグ･レベルのメッセージ**

コマンドボタン

Apply - IBP を入力値で更新する。

8.2.6.4　ホストを構成する

ログ化メッセージをホストに送るように構成できる。

Configuration		
Buffered Log / Command Logger / Console Log / Hosts / Syslog		
Host:	Add	
IP Address:*	. . .	
* = mandatory		
	Apply	Refresh

図: ロギング･ホスト･コンフィグ

選択基準

Host/ホスト - シスログ用に構成されたホストのリストである。 構成を変更するホストを選択する、または、ドロップダウン･リストから新たなホストを追加する。

Severity Filter/重大度 -ログは構成された重大度閾値に等しいまたはそれを超えるメッセージを記録する。 重大度オプションはプルダウン入力欄の該当行を選択して選択する。 これらの重大度レベルを次に列挙した：

- Emergency/緊急 (0): システムは使用不可
- Alert/アラート (1): 直ちにアクションを要する
- Critical/致命的 (2): 致命的な状況
- Error/エラー (3): エラー状況
- Warning/警告 (4): 警戒を要する状況
- Notice/注意(5): 通常ではあるが重要な状況
- nformational/情報提供(6): 情報提供のみのメッセージ
- Debug/デバッグ(7): デバッグ･レベルのメッセージ

構成可能データ

IP Address/IPアドレス - シスログ用に構成されたホストのIPアドレスである。

Port /ポート - シスログ･メッセージが送られるホストのポートである。 デフォルト･ポートは514である。テキスト欄にポートを指定する。

構成不可能なデータ

Status/ステータス - これはホストがアクティブにロギングするかを指定する。

コマンドボタン

Apply - IBP を入力値で更新する。

Refresh/更新-データベースを再取得して、テーブルの最初のエントリから始めて再表示する。

Delete/削除 - 構成されたホストを削除する。

© 2010 富士通テクノロジー･ソリューションズ

8.2.6.5 シスログを構成する

システムでシスログ･システムを有効化するには、ログ化メッセージが"ホスト"頁で指定されたホストに送られる。

Configuration

Buffered Log | Command Logger | Console Log | Hosts | Syslog

Admin Status: Disable
Local UDP Port (1 to 65535) :* 514
Messages Received: 16
Messages Dropped: 0
Messages Relayed: 0
* = mandatory

Apply Refresh

図：シスログ･コンフィグ

選択基準

管理ステータス - 構成されたシスログ･ホストへのロギングを有効化/無効化するためにある これを無効化するするとすべてのシスログ･ホストへのロギングを停止する。 無効化とはここでどのコレクタ/リレーにもメッセージが送られないことを意味する。 有効化とはコレクタ/リレー毎に構成された値で構成されたコレクタ/リレーにメッセージが送られることを意味する。 シスログ機能の動作の有効化と無効化はプルダウン入力欄の該当行を選択する。

構成可能データ

ローカルUDPポート - シスログ･メッセージを送り出すローカル･ホストのポートである デフォルト･ポートは514である。テキスト欄にローカル･ポートを指定する。

構成不可能なデータ

受信メッセージ - ログ･プロセスにより受信されたメッセージ数 これには落とされたり無視されたメッセージも含む。

落とされたメッセージ - エラーまたはリソース不足のためプロセスできなかったメッセージ数

中継されたメッセージ - シスログ機能によりシスログ･ホストへ転送たメッセージ数 複数のホストに転送されたメッセージはホスト毎に一回計数される。

コマンドボタン

Apply - IBP を入力値で更新する。

Refresh/更新- データベースを再取得して、テーブルの最初のエントリから始めて再表示する。.

8.2.6.6　バッファー・ログを見る

バッファー・ログ、持続的ログ、またはコンソール・ログに表示されたすべてのログ化メッセージの形式にメッセージを適用するのに役立つ。

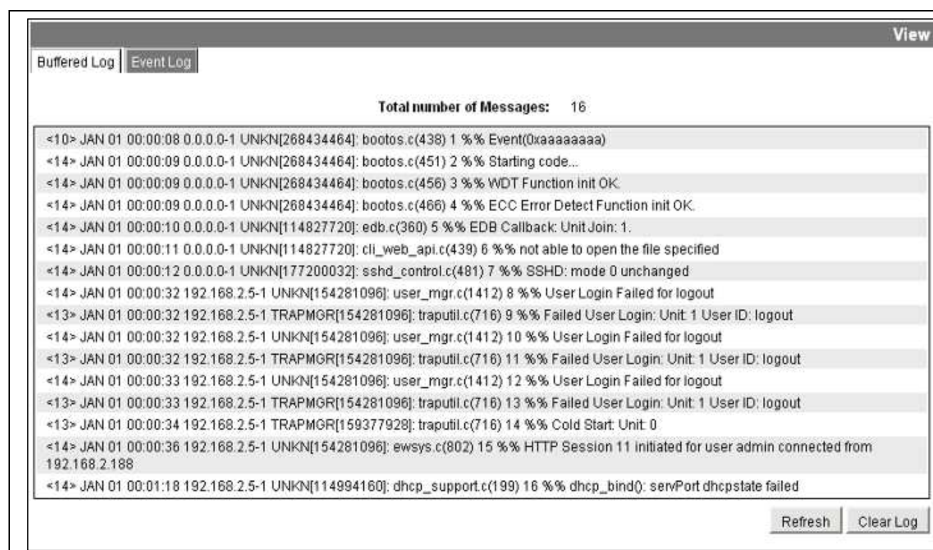


図 :バッファー・ログを見る

メッセージの形式

シスログを通してコレクタまたはリレーにログ化されたメッセージは同一形式である：

<15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry（メッセージ・エイジ時間の終了にともないインターフェイス12はルート・ステートに移行した）

- 上の例は、8月24日5時34分5秒付ファイルmstp_api.cの318行にあるスレッドIDが2110で実行中のコンポーネントMSTPにより生成されたシステムに重大度7(15 mod 8)（デバッグ)によるメッセージを示す。これはシステムIP0.0.0.0で装置番号1によるログ化された237番目のメッセージである。

表示されたログ・メッセージ数: バッファー・ログではウェブ頁には最新の128エントリまでのみ表示される。

コマンドボタン

Refresh/更新 - 頁を最新ログ・エントリで更新する。

Clear Log/ログをクリアする - ログ内すべてのエントリを消去する。

8.2.6.7　　イベント･ログを見る

このパネルを使用してイベント･ログを表示する。破壊的イベント用エラー･メッセージを保持するために使用される。 イベントがログ化され、更新ログがフラッシュ･メモリに保存されてから、IBPはリセットされる。 ログは少なくとも10,080エントリを保持でき(実際の数はプラットフォームとOSに依存する)、容量が最大になってからエントリを追加しようとすると消去される。 イベント･ログはシステム･リセット後でも保持される。

View

Buffered Log | Event Log

Entry		Filename	Line	TaskID	Code	Time
00001:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00002:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00003:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00004:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00005:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00006:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00007:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00008:	EVENT>	bootos.c	438	0FFFFC20	AAAAAAAA	1970/01/01 00:00:08
00009:	EVENT>	log_extend.c	732	09232D20	AAAAAAAA	1970/01/01 09:56:35

Refresh | Clear Log

図 ： イベント･ログを見る

構成不可能なデータ

Entry/エントリ - イベント･ログ内のエントリ数 最新エントリが先頭に来る。

Filename/ファイル名 - イベントを検出したコードを識別するソース･コードのファイル名。

Line/行 - イベントを検出したコードのソース･ファイル内の行番号。

Task ID/タスクID - イベントを報告するタスクのOSが割当てるID。

Code/コード - イベントを報告するコードによるイベント･ログ･ハンドラに渡されるイベント･コード。

Time/時間 - 直前リセット時点から起算したイベント発生時の時間。

コマンドボタン

Refresh/更新 - 頁を最新ログ･エントリで更新する。

Clear Log/ログをクリアする - ログ内すべてのエントリを消去する。

© 2010 富士通テクノロジー･ソリューションズ

8.2.7　統計

8.2.7.1　スイッチ・サマリ

Statistics

Switch Summary | Switch Detailed | Port Summary | Port Detailed

ifIndex:	49
Total Packets Received without Errors:	0
Broadcast Packets Received:	0
Packets Received with Errors:	0
Packets Transmitted without Errors:	2
Broadcast Packets Transmitted:	0
Transmit Packet Errors:	0
Address Entries Currently in Use:	1
VLAN Entries Currently in Use:	5
Time Since Counters Last Cleared:	0 day 0 hr 5 min 36 sec

Clear Counters　Refresh

図 : IBP概観統計

構成不可能なデータ

ifIndex - IBPのプロセッサと関連付けられたインターフェイス・テーブル・エントリのインターフェイス番号を示すオブジェクトである。

Packets Received Without Errors/エラー無しで受信されたパケット - プロセッサに受信されたパケット総数（ブロードキャスト・パケットとマルチキャスト・パケットを含む）

Broadcast Packets Received/受信されたブロードキャスト・パケット - ブロードキャスト・アドレスにダイレクトされた受信パケット総数、 これにはマルチキャスト・パケットが含まれないことに注意する。

Packets Received With Error/ エラー有りで受信されたパケット - エラーのため受信できなかったパケット数

Packets Transmitted Without Errors/エラー無しで送信されたパケット - インターフェイスから送信されたパケット総数

Broadcast Packets Transmitted/送信されたブロードキャスト・パケット - エラーのため送信できなかったパケット総数。

Transmit Packet Errors/送信パケット・エラー - エラーのため送信できなかったアウトバウンド・パケット数

Address Entries Currently in Use/現在使用中のアドレス・エントリ - 学習されたエントリと静的エントリを含み、IBPで現在の転送データベース・アドレス・テーブルのエントリ総数

VLAN Entries Currently in Use/現在使用中のVLANエントリ - VLANテーブルを現在占有するVLANエントリ数

Time Since Counters Last Cleared/直前にカウンターがクリアされてからの時間 - IBPの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒までで示したもの。

コマンドボタン

Clear Counters/カウンター消去 - すべてのサマリとIBPの詳細統計をデフォルト値に戻す、すべてのカウンター消去。 消去されたパケット数はクリアできない。

Refresh/更新 - IBPにある現在のデータ・ステートにより画面のデータを更新する。

8.2.7.2　　スイッチの詳細

Statistics

Switch Summary | Switch Detailed | Port Summary | Port Detailed

ifIndex:	49
Octets Received:	0
Packets Received Without Error:	0
Unicast Packets Received:	0
Multicast Packets Received:	0
Broadcast Packets Received:	0
Receive Packets Discarded:	0
Octets Transmitted:	188
Packets Transmitted without Errors:	2
Unicast Packets Transmitted:	0
Multicast Packets Transmitted:	2
Broadcast Packets Transmitted:	0
Transmit Packets Discarded:	0
Most Address Entries Ever Used:	1
Address Entries in Use:	1
Maximum VLAN Entries:	3965
Most VLAN Entries Ever Used:	5
Static VLAN Entries:	5
Dynamic VLAN Entries:	0
VLAN Deletes:	0
Time Since Counters Last Cleared:	0 day 0 hr 5 min 54 sec

Clear Counters　Refresh

図：IBP詳細統計

構成不可能なデータ

ifIndex - IBPのプロセッサと関連付けられたインターフェイス・テーブル・エントリのインターフェイス番号を示すオブジェクトである。

Octets Received/受信されたオクテット - プロセッサにより受信されたデータ・オクテット総数（フレーム・ビットを除きFCSオクテットを含む）。

Packets Received Without Errors/エラー無しで受信されたパケット - プロセッサに受信されたパケット総数（ブロードキャスト・パケットとマルチキャスト・パケットを含む）

Unicast Packets Received/受信ユニキャスト・パケット - 高レイヤー・プロトコルにデリバリされたサブネットワーク・ユニキャスト・パケット数

Multicast Packets Received/受信マルチキャスト・ パケット - マルチキャスト・アドレスにダイレクトされた受信パケット総数 この総数にはブロードキャスト・アドレスにダイレクトされたパケットは含まれないことに注意する。

Broadcast Packets Received/受信されたブロードキャスト・パケット - ブロードキャスト・アドレスにダイレクトされた受信パケット総数、 これにはマルチキャスト・パケットが含まれないことに注意する。

Receive Packets Discarded/廃棄された受信パケット - エラーのため受信できなかったパケット数。

Octets Transmitted/送信されたオクテット - インターフェイスから送信された、フレーム文字を含むオクテット総数

Packets Transmitted Without Errors/エラー無しで送信されたパケット - インターフェイスから送信されたパケット総数

Unicast Packets Transmitted/ 送信されたユニキャスト・パケット - 高レイヤー・プロトコルにサブネットワーク・ユニキャスト・アドレスへの送信を要求されたパケット総数で破棄されたものも含む

Multicast Packets Transmitted/ 送信されたマルチキャスト・パケット - 高レイヤー・プロトコルにマルチキャスト・アドレスへの送信を要求されたパケット総数で破棄されたものも送られなかったものも含む

Broadcast Packets Transmitted/ 送信されたブロードキャスト・パケット - 高レイヤー・プロトコルにブロードキャスト・アドレスへの送信を要求されたパケット総数で破棄されたものも送られなかったものも含む。

Transmit Packets Discarded/廃棄された送信パケット - エラーのため送信できなかったパケット数。 パケット廃棄の考えうる理由はバッファー容量を空けるため。

Most Address Entries Ever Used/使用された最大アドレス・エントリ - 直前の再起動以降IBPが学習した転送データベース・アドレス・テーブルのエントリの最大数

Address Entries in Use/使用中アドレス・エントリ - 当該IBPの転送データベース・アドレス・テーブルにある学習エントリと静的エントリの数

Maximum VLAN Entries/最大VLANエントリ - IBPで許可された仮想LAN (VLANs) の最大数

Most VLAN Entries Ever Used/使用された最大VLANエントリ - 直前再起動以降このIBPでアクティブなVLANの最大数

Static VLAN Entries/静的VLANエントリ - このIBPにある静的に生成された現在アクティブなVLANエントリ数

VLAN Deletes/削除されたVLAN - 直前再起動以降生成され、削除されたこのIBPにあるVLANの数

Time Since Counters Last Cleared/カウンターの直前クリア以降の経過時間 - このIBPの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒までで示したもの

コマンドボタン

Clear Counters/カウンター消去 - すべてのサマリとIBPの詳細統計をデフォルト値に戻す、すべてのカウンター消去 消去されたパケット数はクリアできない。

Refresh/更新 - IBPにある現在のデータ・ステートにより画面のデータを更新する。

© 2010 富士通テクノロジー・ソリューションズ

8.2.7.3　ポート･サマリ

Statistics

Switch Summary | Switch Detailed | Port Summary | Port Detailed

Slot/Port:	Encl-CB1/0/1
ifIndex:	1
Total Packets Received without Errors:	0
Packets Received with Errors:	0
Broadcast Packets Received:	0
Packets Transmitted without Errors:	0
Transmit Packet Errors:	0
Collision Frames:	0
Time Since Counters Last Cleared:	0 day 0 hr 6 min 6 sec

Clear Counters | Clear All Counters | Refresh

図 : ポート･サマリ統計

選択基準

Slot/Port / スロット/ポート - データが表示されるまたは構成されるインターフェイスを選択する

構成不可能なデータ

ifIndex - アダプタ上でこのポートと関連付けられたインターフェイス･テーブル･エントリのインターフェイス番号を示すオブジェクトである。

Total Packets Received Without Errors/エラー無しで受信されたパケット総数 - エラー無しで受信されたパケット総数

Packets Received With Error/エラー有りで受信されたパケット - エラーのため受信できなかったパケット数

Broadcast Packets Received/受信されたブロードキャスト･パケット - ブロードキャスト･アドレスにダイレクトされた健全な受信パケット総数 これにはマルチキャスト･パケットが含まれないことに注意する。

Packets Transmitted Without Errors/エラー無しで送信されたパケット - このポートによりセグメントへ送信されたフレーム数

Transmit Packet Errors/送信パケット･エラー - エラーのため送信できなかったアウトバウンド･パケット数

Collision Frames/コリジョン･フレーム - 当該イーサネット･セグメントでのコリジョン総数

Time Since Counters Last Cleared/カウンターの直前クリア以降の経過時間 - このポートの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒までで示したもの。

コマンドボタン

Clear Counters - このポートのすべての統計をデフォルト値に戻す、すべてのカウンター消去

Clear All Counters - すべてのポートのすべての統計をデフォルト値に戻す、すべてのポート･カウンターの消去

Refresh/更新 - IBPにある現在のデータ･ステートにより画面のデータを更新する。.

8.2.7.4 ポート詳細

Statistics

Switch Summary | Switch Detailed | Port Summary | Port Detailed

Slot/Port:	Encl-CB1/0/1
ifIndex:	1
Packets RX and TX 64 Octets:	0
Packets RX and TX 65-127 Octets:	0
Packets RX and TX 128-255 Octets:	0
Packets RX and TX 256-511 Octets:	0
Packets RX and TX 512-1023 Octets:	0
Packets RX and TX 1024-1518 Octets:	0
Packets RX and TX 1519-2047 Octets:	0
Packets RX and TX 2048-4095 Octets:	0
Packets RX and TX 4096-9216 Octets:	0
Octets Received:	0
Packets Received 64 Octets:	0
Packets Received 65-127 Octets:	0
Packets Received 128-255 Octets:	0
Packets Received 256-511 Octets:	0
Packets Received 512-1023 Octets:	0
Packets Received 1024-1518 Octets:	0
Packets Received > 1522 Octets:	0
Total Packets Received without Errors:	0
Unicast Packets Received:	0
Multicast Packets Received:	0
Broadcast Packets Received:	0
Total Packets Received with MAC Errors:	0
Jabbers Received:	0
Undersize Received:	0
Fragments Received:	0
Alignment Errors:	0
Rx FCS Errors:	0
Overruns:	0

図：ポート詳細統計

選択基準

Slot/Port - データが表示されるまたは構成されるインターフェイスを選択する

構成不可能なデータ

ifIndex - アダプタ上でこのポートと関連付けられたインターフェイス・テーブル・エントリのインターフェイス番号を示すオブジェクトである。

Packets RX and TX 64 Octets/64オクテットの送受信パケット - 長さ64オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 65-127 Octets/65~127オクテットの送受信パケット - 長さ65と127オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 128-255 Octets /28-255オクテットの送受信パケット - - 長さ128と255オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 256-511 Octets 256-511オクテットの送受信パケット -

長さ256と511オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 512-1023 Octets - 512-1023オクテットの送受信パケット -

長さ512と1023オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 1024-1518 Octets - 1024-1518 オクテットの送受信パケット -

長さ1024と1518オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 1519-2047 Octets - 1519-2047 オクテットの送受信パケット -

長さ1519と2047 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 2048-4095 Octets - 2048-4095オクテットの送受信パケット -

長さ2048 と4095 オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 4096-9216 Octets - 4096-9216 オクテットの送受信パケット -

長さ4096と9216オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Octets Received/受信オクテット - ネットワークで受信された(失敗したパケットにあるものを含む)データ・オクテット総数 (フレーム・ビットを除きFCSオクテットを含む)。 このオブジェクトはイーサネット使用度の適度な推計値として使用できる。 より高精度が必要な場合、etherStatsPktsとetherStatsOctetsオブジェクトが共通間隔の前後にサンプルされる必要がある。

Packets Received 64 Octets /64オクテットの受信パケット - 長さ64オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 65-127 Octets / 65-127オクテットの受信パケット-長さ65と127オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 128-255 Octets / 128-255オクテットの受信パケット-

長さ128と255オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 256-511 Octets / 256-511オクテットの受信パケット-

長さ256と511オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 512-1023 Octets / 512-1023オクテットの受信パケット-

長さ512と1023オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 1024-1518 Octets / 1024-1518オクテットの受信パケット -

長さ1024と1518オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received > 1522 Octets - 長さ1522オクテット以上の受信され(フレーム・ビットを除きFCSオクテットを含む).、良好に形成されたパケット総数(失敗したパケットを含む)。

Total Packets Received Without Errors - エラー無しで受信されたパケット総数。

Unicast Packets Received/受信ユニキャスト・パケット - 高レイヤー・プロトコルにデリバリされたサブネットワーク・ユニキャスト・パケット数。

Multicast Packets Received/受信マルチキャスト・ パケット - マルチキャスト・アドレスにダイレクトされた健全な受信パケット総数 この総数にはブロードキャスト・アドレスにダイレクトされたパケットは含まれないことに注意する。

Broadcast Packets Received/受信ブロードキャスト・ パケット - ブロードキャスト・アドレスにダイレクトされた健全な受信パケット総数 これにはマルチキャスト・パケットが含まれないことに注意する。

© 2010 富士通テクノロジー・ソリューションズ

Total Packets Received with MAC Errors/MACエラー有りで受信されたパケット総数 - エラーのため受信できなかったパケット総数

Jabbers Received/受信ジャバー

長さ1518オクテット以上の受信され(フレーム・ビットを除きFCSオクテットを含む)、良好に形成され、さらにオクテットの整数倍による失敗したフレーム・チェック・シーケンス(FCSエラー)またはオクテットの非整数倍による失敗したFCS(アラインメント・エラー)があるパケット総数 このジャバー定義はIEEE-802.3 セクション8.2.1.5 (10BASE5) とセクション10.3.1.4 (10BASE2)の定義とは異なる。 この文書ではジャバーをパケットが20msを超える条件として定義する。ジャバー検出許容範囲は20msから150msである。

Undersize Received/受信アンダーサイズ・パケット - 64オクテット未満の受信され(フレーム・ビットを除きFCSオクテットを含む)、良好なCRCによるパケット総数

Fragments Received/受信断片 - 64オクテット未満の受信され(フレーム・ビットを除きFCSオクテットを含む)、CRCエラーがあるパケット総数

Alignment Errors/アラインメント・エラー - 長さ64オクテット以上1518オクテット以下の受信され(フレーム・ビットを除きFCSオクテットを含む)、 オクテットの非整数倍による失敗したフレーム・チェック・シーケンス（FCS）があるパケット総数

Rx FCS Errors/受信FCSエラー - 長さ64オクテット以上1518オクテット以下の受信され(フレーム・ビットを除きFCSオクテットを含む)、 オクテットの整数倍による失敗したフレーム・チェック・シーケンス（FCS）があるパケット総数

Overruns/オーバーラン - このポートが受信パケットにより過負荷状態となり、流入パケットに対応できなくなったために破棄されたフレーム総数

Total Packets Transmitted (Octets) /送信されたパケット総数- ネットワークで送信された(失敗したパケットにあるものを含む)データ・オクテット総数 (フレーム・ビットを除きFCSオクテットを含む). このオブジェクトはイーサネット使用度の適度な推計値として使用できる。 より高精度が必要な場合、etherStatsPktsとetherStatsOctetsオブジェクトが共通間隔の前後にサンプルされる必要がある。

PacketsTransmitted 64 Octets /送信された64オクテット・パケット- 長さ64オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。 .

Packets Transmitted 65-127 Octets /送信された65-127オクテット・パケット-長さ65と127オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 128-255 Octets /送信された128-255オクテット・パケット--長さ128と255オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 256-511 Octets /送信された256-511オクテット・パケット-- 長さ256と511オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 512-1023 Octets /送信された128-255オクテット・パケット -長さ512と1023オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 1024-1518 Octets /送信された1024-1518オクテット・パケット-- 長さ1024と1518オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Maximum Frame Size/最大フレーム・サイズ - イーサネット・ヘッダー、CRC、ペイロードを含みインターフェイスがサポートするまたは構成された最大イーサネット・フレーム・サイズ --> (1518 to 9216). デフォルト最大フレーム・サイズは1518である。

Total Packets Transmitted Successfully/送信成功パケット総数 - インターフェイスから送信されたパケット総数。

Unicast Packets Transmitted/送信されたユニキャスト・ パケット -高レイヤー・プロトコルにサブネットワーク・ユニキャスト・アドレスへの送信を要求されたパケット総数で破棄されたものも送られなかったものも含む。

© 2010 富士通テクノロジー・ソリューションズ

Multicast Packets Transmitted/送信されたマルチキャスト・ パケット-高レイヤー・プロトコルにマルチキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む。

Broadcast Packets Transmitted/送信されたブロードキャスト・ パケット - エラーのため送信できなかったパケット総数。

Total Transmit Errors/合計送信エラー - シングル、マルチ、エクセシブ・コリジョンの合計値

Tx FCS Errors/送信FCSエラー - 長さ64オクテット以上1518オクテット以下の送信され(フレーム・ビットを除きFCSオクテットを含む)。、 オクテットの整数倍による失敗したフレーム・チェック・シーケンス (FCS) があるパケット総数。

Underrun Errors/アンダーラン・エラー - 送信FIFOバッファーがフレーム送信中に空になったため破棄されたフレーム総数

Total Transmit Packets Discarded/破棄された合計送信パケット - 破棄されたシングル・コリジョン・フレーム、破棄されたマルチ・コリジョン・フレーム、破棄されたエクセシブ・フレームの合計値。

Single Collision Frames/シングル・コリジョン・フレーム - 送信がちょうどコリジョン1回で妨害された特定インターフェイス上で送信が完了したフレーム数。

Multiple Collision Frames/マルチ・コリジョン・フレーム - 送信が1回以上のコリジョンで妨害された特定インターフェイス上で送信が完了したフレーム数。

Excessive Collision Frames/過度コリジョン・フレーム - 過度のコリジョンにより特定インターフェイスでの送信障害を起こしたフレーム数

Time Since Counters Last Cleared/カウンターの直前クリア以降の経過時間 - このポートの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒までで示したもの

コマンドボタン

Clear Counters - このポートのすべての統計をデフォルト値に戻す、すべてのカウンター消去

Clear All Counters -すべてのポートのすべての統計をデフォルト値に戻す、すべてのポート・カウンターの消去

Refresh/更新 - IBPにある現在のデータ・ステートにより画面のデータを更新する。.

8.2.8 SNMP

8.2.8.1 コミュニティー・コンフィグ

デフォルトでは2個のSNMPコミュニティーがある：

- プライベート。'Read・Write'特権とステータスが有効化に設定されている。
- パブリック。'Readのみ'特権とステータスが有効化に設定されている。

これらは周知のコミュニティーであり、このメニューからデフォルトを変更したり他のコミュニティーを追加できる。このメニューから定義するコミュニティーにみSNMPv1とSNMPv2cプロトコルでIBPにアクセスできる。 読み・書きアクセス特権があるコミュニティーのみこのメニューにSNMPによりアクセスできる。

SNMPv1とSNMPv2cプロトコルを使用するときはこのメニューを使用しなければならない。 SNMP v3を使用する場合、ユーザー・アカウント・メニューを使用する。

SNMP

Community Config | Trap Receiver Config | Trap Flags | Trap Log | Supported MIBs

Community: public
SNMP Community Name:* public
Client IP Address:* 0 . 0 . 0 . 0
Client IP Mask:* 0 . 0 . 0 . 0
Access Mode: Read Only
Status: Enable
* = mandatory

Apply Delete

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
private	0.0.0.0	0.0.0.0	Read/Write	Enable

図：SNMPコミュニティー・コンフィグ

選択基準

Community/コミュニティー - 存コミュニティーを再構成する、または新たなアカウントを生成するにはこの画面を使用できる。 このプルダウン・メニューから既存コミュニティーの名前を選択する、または'Create'を選択して新たなコミュニティーを追加できる。

Access Mode/アクセス・モード –

プルダウン・メニューから読み・書きまたは読みのみを選択してこのコミュニティーのアクセスレベルを指定する

Status/ステータス - プルダウン・メニューから有効化または無効化を選択してこのコミュニティーのステータスを指定する 有効化を選択すると、コミュニティー名はすべての有効なコミュニティー名に固有でなければならない。さもないと設定要求は拒否される。 無効化を選択すると、コミュニティー名は無効化される。

構成可能データ

SNMP Community Name/ SNMP コミュニティー名- SNMPコミュニティー名であり、SNMPコミュニティー間を識別する。 SNMPコミュニティー内のコミュニティー名は固有でなければならない。 有効な入力は最大16文字までの大文字と小文字が区別される文字列である。

Client IP Address/クライアントIPアドレス - クライアントIPアドレスとクライアントIPマスクはまとめ、そこからSNMPクライアントが当該コミュニティーを使用してこの装置にアクセスできるIPアドレスの範囲を指す。IPアドレスまたはIPマスクの値が0.0.0.0の場合、任意のIPアドレスからアクセスできる。 それ以外の場合、各クライアントのIPアドレスはクライアントIPアドレスがそうであるように、マスクと結合され、また、各値が等

しい場合、アクセスは許可される。 たとえば、クライアントIPアドレスとクライアントIPマスク・パラメータが192.168.1.0/255.255.255.0の場合、IPアドレスが192.168.1.0から192.168.1.255までのどのクライアントからでもアクセスできる。 1台のみのワークステーションからアクセスを許可する場合、クライアントIPマスク値を255.255.255.25とし、当該マシンのIPアドレスをクライアントIPアドレスに使用する。

Client IP Mask/クライアントIPマスク - クライアントIPアドレスとクライアントIPマスクはまとめ、そこからSNMPクライアントが当該コミュニティーを使用してこの装置にアクセスできるIPアドレスの範囲を指す。 IPアドレスまたはIPマスクの値が0.0.0.0の場合、任意のIPアドレスからアクセスできる。 それ以外の場合、各クライアントのIPアドレスはクライアントIPアドレスがそうであるように、マスクと結合され、また、各値が等しい場合、アクセスは許可される。 たとえば、クライアントIPアドレスとクライアントIPマスク・パラメータが192.168.1.0/255.255.255.0の場合、IPアドレスが192.168.1.0から192.168.1.255までのどのクライアントからでもアクセスできる。 1台のみのワークステーションからアクセスを許可する場合、クライアントIPマスク値を255.255.255.25とし、当該マシンのIPアドレスをクライアントIPアドレスに使用する。

コマンドボタン

Apply - IBP を画面の値で更新する。. IBPにパワー・サイクル後、保持させるには、保存を実行しなければならない。

Delete/削除-現在選択されているコミュニティー名を削除する。 IBPにパワー・サイクル後、保持させるには、保存を実行しなければならない。.

8.2.8.2 トラップ･レシーバー･コンフィグ

このメニューはアクティブなトラップ･レシーバー毎にエントリを表示する。

図 ：SNMP トラップ･レシーバー･コンフィグ

選択基準

Community/コミュニティー - 既存コミュニティーを再構成する、または新たなアカウントを生成するにはこの画面を使用できる。 このプルダウン･メニューから既存コミュニティーの名前を選択する、または'Create'を選択して新たなコミュニティーを追加できる。

SNMP Version - プルダウン･メニューからレシーバーが使用するトラップ･バージョンを選択する：

- SNMP v1 - SNMP v1 を使用してトラップをレシーバーに送る
- SNMP v2 - SNMP v2 を使用してトラップをレシーバーに送る

ステータス - プルダウン･メニューからレシーバーのステータスを選択する：

- 有効化 - トラップをレシーバーに送る
- 無効化 - トラップをレシーバーに送らない

構成可能データ

SNMP Community Name/SNMP コミュニティー名 - SNMPトラップ･パケットがトラップ･マネージャに送られるようにコミュニティー文字列を入力する 最大16文字で大文字と小文字は区別される。

IP Address/ IPアドレス - この装置からSNMPトラップを受信するIPアドレスを入力する。 0から255までの4個の数字をピリオドで区切り入力する。

コマンドボタン

Apply - IBP を画面の値で更新する。. パワー･サイクル後、新たな値を保持させるには、保存を実行しなければならない。.

Delete/削除- 現在選択されているコミュニティー名を削除する。 パワー･サイクル後、新たな値を保持させるには、保存を実行しなければならない。.

8.2.8.3　トラップ･フラッグ

どのトラップを有効化するか指定するためにこのメニューを使用する。 アクティブ･トラップにより識別される条件にIBPが合致すると、トラップ･メッセージが任意の有効化されたSNMPトラップ･レシーバーに送られ、メッセージがトラップ･ログに書き込まれる。

SNMP

Community Config | Trap Receiver Config | Trap Flags | Trap Log | Supported MIBs

Authentication: Enable
Link Up/Down: Enable
Multiple Users: Enable
ACL Traps : Disable

Apply

図 ：SNMPトラップ･フラッグ

選択基準

Authentication - プルダウン入力欄の対応行を選択して認証失敗トラップを有効化または無効化する。 デフォルト設定は有効化されている。

Link Up/Down - プルダウン入力欄の対応行を選択してリンク･ステータス･トラップを有効化または無効化する。 デフォルト設定は有効化されている。

Multiple Users - プルダウン入力欄の対応行を選択して複数ユーザー･トラップを有効化または無効化する。 デフォルト設定は有効化されている。

このトラップは同じユーザーIDが同じ時、IBPに (Telnetまたはシリアルポート経由で)ログインすると作動する。

ACL Traps - プルダウン入力欄の対応行を選択してACLトラップを有効化または無効化する 工場側デフォルトは無効化されている。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないとパワー･サイクル後、保持されない。

変更は保存を実行しなければパワー･サイクル後、保持されない。

8.2.8.4　トラップ･ログ

この画面はトラップ･ログのエントリをリストする。 システム･ユーティリティー、IBPからアップロードしたファイルを使用してトラップログ情報をファイルとして取得できる。

SNMP

Community Config | Trap Receiver Config | Trap Flags | Trap Log | Supported MIBs

Number of Traps Since Last Reset: 4
Trap Log Capacity: 256
Number of Traps Since Log Last Viewed: 4

Log	System Up Time	Trap
0	1970/01/01 08:00:34	Cold Start: Unit: 0
1	1970/01/01 08:00:33	Failed User Login: Unit: 1 User ID: logout
2	1970/01/01 08:00:32	Failed User Login: Unit: 1 User ID: logout
3	1970/01/01 08:00:32	Failed User Login: Unit: 1 User ID: logout

Clear Log

図 :SNMPトラップ･ログ

構成不可能なデータ

Number of Traps Since Last Reset/最後のリセット以降のトラップ数 - 直前にトラップ･ログ･エントリが生成されてから生成されたトラップ数。

Trap Log Capacity/トラップ･ログ容量 - ログに保存されるトラップの最大数 この容量をトラップ数が超過すると、エントリは古いエントリ順に上書きする。

Number of Traps since log last viewed/最後の閲覧以降のトラップ数 - 直前にトラップが表示されて以降発生したトラップ数。 どの方法(端末インターフェイス･ディスプレイ、ウェブ･ディスプレイ、IBPからのアップロード･ファイル等)を用いてもトラップを表示するとこのカウンターは0にリセットされる。

Log/ログ- このトラップのシーケンス番号

System Up Time/システム稼働時間 - IBP.を最後に再起動して以降経過した日数、時間、分、秒で表現される当該トラップの発生時間

Trap/トラップ - トラップの識別情報

コマンドボタン

Clear Log/ログをクリアする - ログ内すべてのエントリを消去する。 この後にログを表示すると新たなログ･エントリのみ表示される。

8.2.8.5　サポートされるMIB

これはIBPがサポートするすべてのMIBのリストである。

SNMP

Community Config | Trap Receiver Config | Trap Flags | Trap Log | Supported MIBs

Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
FSC-SWITCH-MIB	Fujitsu Siemens Computers Reference
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-TARGET-MIB	The Target MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB	SNMP Research, Inc.
LAG-MIB	The Link Aggregation module for managing IEEE 802.3ad
RFC 1213 - RFC1213-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1493 - BRIDGE-MIB	Definitions of Managed Objects for Bridges (dot1d)
RFC 2674 - P-BRIDGE-MIB	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.
RFC 2674 - Q-BRIDGE-MIB	The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks
RFC 2737 - ENTITY-MIB	Entity MIB (Version 2)
RFC 2863 - IF-MIB	The Interfaces Group MIB using SMIv2
RFC 3635 - Etherlike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types
SWITCHING-MIB	Switching - Layer 2
SWITCHING-EXTENSION-MIB	Switching extension - Layer 2
INVENTORY-MIB	Unit and Slot configuration.
PORTSECURITY-PRIVATE-MIB	Port Security MIB.
IEEE8021-PAE-MIB	Port Access Entity module for managing IEEE 802.1X.
TACACS-MIB	TACACS MIB
RADIUS-CLIENT-PRIVATE-MIB	Radius MIB
RADIUS-ACC-CLIENT-MIB	RADIUS Accounting Client MIB

図：SNMPがサポートするMIB

構成不可能なデータ

Name - 該当する場合はRFC番号、およびMIB名

Description/内容 - RFCの表題またはMIBの内容

コマンドボタン

Refresh - データを更新する

8.2.9 SNTP

8.2.9.1 グローバル･コンフィグ

図 : SNTP グローバル･コンフィグ

選択基準

Client Mode - SNTPクライアントの動作モードを指定する SNTPクライアントは次のモードのいずれかで動作する。 デフォルト値は"無効化"である。

- ***Disable***- SNTPは動作しない クライアントからSNTP要求が送信されなかった、または、受信されたSNTPメッセージが処理されなかった。
- ***Unicast***- SNTPは2点間で動作する ユニキャスト･クライアントはユニキャスト･アドレスで指定サーバに要求を送り、応答を予期する、この応答によりクライアントは時間を決定し、オプションとしてはサーバとの往復遅延時間とローカル･クロックのオフセットを決めることができる。
- ***Broadcast*** - SNTP はマルチキャスト･モードと同じ動作をするが、マルチキャスト･アドレスではなくローカルのブロードキャスト･アドレスを使用する。 ブロードキャスト･アドレスは1個のサブネット･スコープを持つが、マルチキャスト･アドレスはインターネット全体のスコープがある。

構成可能データ

Port - 応答/ブロードキャストを聞くローカルUDP ポートを指定する 許可範囲は1から65,535である。 デフォルト値は123である。

Unicast Poll Interval - ユニキャスト･モードに構成された場合2の倍数である、ユニキャスト･ポル要求間隔秒数を指定する 許可範囲は6から10である。 デフォルト値は6である。

Broadcast Poll Interval - ブロードキャスト･モードに構成された場合2の倍数で表現される、ブロードキャスト･ポル要求間隔秒数を指定する この間隔が経過する前に受信されたブロードキャストは破棄される。 許可範囲は6から10である。 デフォルト値は6である。

Unicast Poll Timeout - ユニキャスト･モードに構成された場合SNTP応答までの待機秒数を指定する 許可範囲は1から30である。 デフォルト値は5である。

Unicast Poll Retry - ユニキャスト･モードに構成された場合次の構成されたサーバの使用を試行するまでに、最初のタイムアウトからSNTPサーバに要求を再試行する回数を指定する 許可範囲は0から10である。 デフォルト値は1である。

コマンドボタン

Apply -更新された構成をIBPに設定する。 構成変更は直ちに反映される。

© 2010 富士通テクノロジー･ソリューションズ

8.2.9.2　グローバル･ステータス

SNTP

Global Config | Global Status | Server Config | Server Status | Current Time | Time Zone Settings

Version:	4
Supported Mode:	Unicast & Broadcast
Last Update Time:	JAN 01 00:00:00 1970
Last Attempt Time:	JAN 01 00:00:00 1970
Last Attempt Status:	Other
Server IP Address:	
Address Type:	Unknown
Server Stratum:	0 - Unspecified
Reference Clock Id:	
Server Mode:	Reserved
Unicast Server Max Entries:	3
Unicast Server Current Entries:	0
Broadcast Count:	0

図 : SNTP グローバル･ステータス

構成不可能なデータ

Version / バージョン　 - クライアントがサポートするSNTPバージョンを指定する。

Supported Mode - クライアントがサポートするSNTPモードを指定する。 複数のモードをクライアントがサポートできる。

Last Update Time/最後の更新時間- SNTPクライアントが最後にシステム･クロックを更新したローカル日付時刻 (UTC) を指定する。

Last Attempt Time/最後の試行時間 - 直前のSNTP要求または要求しなかったメッセージの受信時であるローカル日付時刻 (UTC) を指定する。

Last Attempt Status/最後の 試行ステータス - ユニキャストとブロードキャスト･モードに対して直前のSNTP要求または要求しなかったメッセージのステータスを指定する。 サーバからメッセージが受信されない場合、Otherのステータスが表示される。 これらの値はすべての動作モードに適格である。

- ***Other*** - 次の列挙値のいずれでもない場合。
- ***Success*** - SNTP動作は成功した、システム時間は更新された。
- ***Request Timed Out*** - SNTPサーバから応答を受信しないダイレクトされたSNTP要求タイムアウト。
- ***Bad Date Encoded*** - SNTPサーバによる時間が有効ではない。
- ***Version Not Supported*** – サーバがサポートするSNTPバージョンはクライアントがサポートするバージョンと互換性が無い。
- ***Server Unsynchronized*** - SNTPサーバがピアと同期化されていない。 これはSNTPメッセージの'leap indicator' 欄に表示される。
- ***Server Kiss Of Death*** - SNTPサーバがこのサーバにはクエリーを送信止めるよう指示した。 これはサーバから受けたメッセージで層欄が 0 であることにより示される。

Server IP Address / サーバIP アドレス　直前に受信された有効なパケットにサーバのIPアドレスを指定する。 どのサーバからもメッセージが受信されなかった場合、空白が表示される。

Address Type - 直前に受信された有効なパケットについてSNTPサーバのアドレス･タイプを指定する。

Server Stratum - 直前に受信された有効なパケットについてサーバの要求層を指定する。

Reference Clock Id - 直前に受信された有効なパケットについてサーバの参照クロック識別子を指定する。

Server Mode - 直前に受信された有効なパケットについてサーバのモードを指定する。

Unicast Sever Max Entries - このクライアントに構成可能なユニキャスト・サーバ・エントリの最大数を指定する。

Unicast Server Current Entries - このクライアントに構成された現在のユニキャスト・サーバ・エントリ数を指定する。

Broadcast Count - 直前の再起動以降SNTPクライアントにより受信され処理された要求しなかったブロードキャストSNTPメッセージ数を指定する。

© 2010 富士通テクノロジー・ソリューションズ

8.2.9.3　　サーバ·コンフィグ

Global Config	Global Status	Server Config	Server Status	Current Time	Time Zone Settings

SNTP

Server: Create
IP Address
Port (1 to 65535):* 123
Priority (1 to 3):* 1
Version (1 to 4):* 4
* = mandatory

Apply　Delete

図　:SNTPサーバ·コンフィグ

選択基準

Server - 追加の"Create".オプション付きで既存のサーバ·アドレスをすべて指定する "Create"を選択すると別のテキストボックス"Address"が表示され、ここには構成するサーバのアドレスを入力できる。

Address Type - 構成されたSNTPサーバ·アドレスのアドレス·タイプを指定する 許可されるタイプ:

- IPv4:
- ホスト名

デフォルト値はIPV4である。

構成可能データ

Address - SNTPサーバ·アドレスを指定する これはSNTPサーバのエンコード化ユニキャストIPアドレスかホスト名を含む最大64文字の文字列である。 ユニキャストSNTP要求はこのアドレスに送られる。 このアドレスがDNSホスト名である場合、そのホスト名はSNTP要求が送信される毎にIPアドレスに解決される必要がある。

Port - SNTP要求が送信されるサーバのポートを指定する 許可範囲は1から65,535である。 デフォルト値は123である。

Priority/プライオリティ - SNTP要求が送られるサーバ·シーケンスを決めるこのサーバ·エントリのプライオリティを指定する クライアントは応答受信に成功するかすべてのサーバに要求を処理させるまでは異なるサーバに要求を送り続ける。 このオブジェクトはサーバ·クエリーを行う順番を示す。 プレシデンスが1のサーバ·エントリはプライオリティが2のサーバより先にクエリーを行われる。 1個以上のサーバが同じプライオリティを持つ場合、要求順序はこのテーブルにあるエントリの辞書的順序に従う。 許可範囲は1から3である。 デフォルト値は1である。

Version - サーバで実行されるNTPバージョンを指定する 許可範囲は1から4である。 デフォルト値は4である。

コマンドボタン

Apply -更新された構成をIBP設定する。 構成変更は直ちに反映される。

Delete/削除- SNTPサーバ·エントリを削除する。 更新された構成をIBP設定する。 構成変更は直ちに反映される。

8.2.9.4　サーバ･ステータス

SNTP

Global Config | Global Status | Server Config | Server Status | Current Time | Time Zone Settings

Address: 1.2.3.4
Last Update Time:
Last Attempt Time: JAN 01 00:00:00 1970
Last Attempt Status: Other
Unicast Server Num Requests: 0
Unicast Server Num Failed Requests: 0

図 : SNTP サーバ･ステータス

構成不可能なデータ

Address/アドレス - 既存のすべてのサーバ･アドレスを指定する サーバ構成が存在しない場合、"No SNTP server exists"メッセージが画面に点滅する。

Last Update Time/最後の更新時間 - 最後にシステム･クロックの更新にこのサーバからの応答が使用されたローカル日付時刻 (UTC) を指定する。

Last Attempt Time/最後の試行時間 - このSNTPサーバが直前にクエリーされたローカル日付時刻 (UTC) を指定する。

Last Attempt Status/最後の 試行ステータス - このサーバへのSNTP要求ステータスを指定する。 このサーバからパケットが受信されない場合、Otherのステータスが表示される。

- ***Other*** - 次の列挙値のいずれでもない場合。
- ***Success*** - SNTP動作は成功した、システム時間は更新された。
- ***Request Timed Out*** - SNTPサーバから応答を受信しないダイレクトされたSNTP要求タイムアウト。
- ***Bad Date Encoded*** - SNTPサーバによる時間が有効ではない。
- ***Version Not Supported*** – サーバがサポートするSNTPバージョンはクライアントがサポートするバージョンと互換性が無い。
- ***Server Unsynchronized*** - SNTPサーバがピアと同期化されていない。 これはSNTPメッセージの 'leap indicator' 欄に表示される。
- ***Server Kiss Of Death*** - SNTPサーバがこのサーバにはクエリーを送信止めるよう指示した。 これはサーバから受けたメッセージで層欄が 0 であることにより示される。

Unicast Server Num Requests/ユニキャスト･サーバ要求回数 - 最後のエージェント再起動以降このサーバに対して行われたSNTP要求回数をを指定する。

Unicast Server Num Failed Requests./ ユニキャスト･サーバ要求失敗回数 - 最後のエージェント再起動以降このサーバに対して行われたSNTP要求の失敗回数をを指定する

8.2.9.5　　現在時刻

SNTP

Global Config | Global Status | Server Config | Server Status | Current Time | Time Zone Settings

Year (2000 - 2099):* 1970
Month (1 - 12):* 1
Day (1 - 31):* 1
Hour (0 - 23):* 8
Minute (0 - 59):* 8
Second (0 - 59):* 42
* = mandatory

Apply

図 ：SNTP現在時刻

構成可能データ

Year /年- 年(4桁). (範囲: 2000 - 2099).

Month - Month. (範囲:: 1 - 12).

Day - 月の日 (範囲: 1 - 31).

Hour - 24時間形式の時間.(範囲: 0 - 23).

Minute - Minute. (範囲: 0 - 59).

Second - Second. (範囲: 0 - 59).

コマンドボタン

Apply - 更新された画面をIBPに設定する。変更はIBPで反映するが保存を実行しないとパワー･サイクル後、保持されなくなる。 .

© 2010 富士通テクノロジー･ソリューションズ

8.2.9.6　時間帯設定

簡易ネットワーク･タイム･プロトコル (SNTP)はIBPがタイム･サーバからの周期的更新に基づいて内部クロックを設定することを可能にする。 IBPに正確な時間を維持すればシステム･ログはイベント･エントリの有意な日付･時刻を記録できる。 CLIを使用しても手動でクロックを設定できる。 クロックが設定されないと、IBPは最後の起動時工場側デフォルト設定からしか時間を記録しない。

図 : SNTP時間帯設定

選択基準

Direction/方向

- before-utc - ローカル時間帯を UTCより先(東側)に設定する。
- after-utc - ローカル時間帯を UTCより後(西側)に設定する。

構成可能データ

Time Zone Name - 時間帯名、通常は略語を用いる (範囲: 1-15 文字).

Time Zone Hours - UTC前後の時間数 (範囲: 0～12 時間).

Time Zone Minutes - UTC前後の分数 (範囲: 0～59 分).

コマンドボタン

Apply - 更新された画面をIBPに設定する。 IBPにパワー･サイクル後も保持させるには保存を実行する。 .

8.2.10 LLDP

8.2.10.1 グローバル・コンフィグ

図 : LLDP グローバル・コンフィグ

構成可能データ

Transmit Interval - LLDPフレームを送信する間隔を秒で指定します。 範囲は1から32768である。 デフォルト値は30秒である。

Hold Multiplier/ホールド乗数 - TTLを割当てる送信間隔に適用される乗数を指定する。 範囲は2から10である。デフォルト値は4である。

Re-Initialization Delay/再初期化遅延 - 再初期化までの遅延時間を指定する。 . 範囲は1から10である。デフォルト値は2 秒である。

Notification Interval/通知間隔 - 通知の送信間隔を秒数で指定する。範囲は5から3600である。デフォルト値は5 秒である。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。

8.2.10.2 インターフェイス・コンフィグ

図 : LLDP インターフェイス・コンフィグ

選択基準

Interface/インターフェイス -LLDP - 802.1ABを構成できるポートのリストを指定する。

Transmit/送信 - 選択されたインターフェイスにLLDP - 802.1ABの送信モードを指定する。

Receive/受信 - 選択されたインターフェイスにLLDP - 802.1ABの受信モードを指定する。

Notify/通知 - 選択されたインターフェイスにLLDP - 802.1ABの通知モードを指定する。

構成可能データ

Transmit Management Information/送信管理情報 - 選択されたインターフェイスについてLLDPフレームで管理アドレスを送信するかを指定する。

Optional TLV(s)/オプションTLV

- **System Name/システム名** - LLDPフレームにシステム名TLVを含む。
- **System Description/システム内容** - LLDPフレームにシステム内容TLVを含む。
- **System Capabilities/システム機能** - LLDPフレームにシステム機能TLVを含む。
- **Port Description/ポート内容** - LLDPフレームにポート内容TLVを含む。

コマンドボタン

Apply -IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。 .

8.2.10.3 インターフェイス・サマリを見る

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Interface	Link Status	Transmit	Receive	Notify	Optional TLV(s)	Transmit Management Information
Encl-CB1/0/1	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/2	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/3	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/4	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/5	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/6	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/7	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/8	Link Down	Enabled	Enabled	Enabled	System Name System Description System Capabilities Port Description	Yes
Encl-CB1/0/9	Link Down	Enabled	Enabled	Enabled	System Name System Description	Yes

図 : LLDP インターフェイス・サマリ

構成不可能なデータ

Interface/インターフェイス - LLDP - 802.1ABを構成できるすべてのポートを指定する。

Link Status/リンク・ステータス - アップリンクかダウンリンクかのポートのリンク・ステータスを指定する。

Transmit/送信- インターフェイスのLLDP - 802.1AB送信モードを指定する。

Receive/受信- インターフェイスのLLDP - 802.1AB受信モードを指定する。

Notify/通知 - インターフェイスのLLDP - 802.1AB通知モードを指定する。

Optional TLV(s)/オプションTLV - 含まれるLLDP - 802.1ABオプションTLVを指定する。

Transmit Management Information/送信管理情報 - LLDPフレームで管理アドレスを送信するかを指定する。

コマンドボタン

Refresh/更新 - ページ情報を更新する。

8.2.10.4 統計を見る

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Last Update: 0 Days 00:00:00
Total Inserts: 0
Total Deletes: 0
Total Drops: 0
Total Ageouts: 0

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unknowns
Encl-CB1/0/1	0	0	0	0	0	0	0
Encl-CB1/0/2	0	0	0	0	0	0	0
Encl-CB1/0/3	0	0	0	0	0	0	0
Encl-CB1/0/4	0	0	0	0	0	0	0
Encl-CB1/0/5	0	0	0	0	0	0	0
Encl-CB1/0/6	0	0	0	0	0	0	0
Encl-CB1/0/7	0	0	0	0	0	0	0
Encl-CB1/0/8	0	0	0	0	0	0	0
Encl-CB1/0/9	0	0	0	0	0	0	0
Encl-CB1/0/10	0	0	0	0	0	0	0
Encl-CB1/0/11	0	0	0	0	0	0	0
Encl-CB1/0/12	0	0	0	0	0	0	0
Encl-CB1/0/13	0	0	0	0	0	0	0
Encl-CB1/0/14	0	0	0	0	0	0	0
Encl-CB1/0/15	0	0	0	0	0	0	0
Encl-CB1/0/16	0	0	0	0	0	0	0
Encl-CB1/0/17	0	0	0	0	0	0	0
Encl-CB1/0/18	0	0	0	0	0	0	0
Encl-CB1/0/19	0	0	0	0	0	0	0
Encl-CB1/0/20	0	0	0	0	0	0	0
Encl-CB1/0/21	0	0	0	0	0	0	0
Encl-CB1/0/22	0	0	0	0	0	0	0
Encl-CB1/0/23	0	0	0	0	0	0	0

図： LLDP 統計

構成不可能なデータ

Last Update/直前の更新 - 遠隔システムと関連付けられたテーブルでエントリが生成、変更、削除された時間を指定する。

Total Inserts/合計挿入数 - 特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが遠隔システムと関連付けられたテーブルに挿入された回数を指定する。

Total Deletes/合計削除数 - 特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが遠隔システムと関連付けられたテーブルから削除された回数を指定する。

Total Drops/合計破棄数 - 特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが遠隔システムと関連付けられたテーブルに入力できなかった回数を指定する。

Total Age outs/合計エイジアウト数 - 特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが、情報タイミング間隔が有効期限を経過したため、遠隔システムと関連付けられたテーブルから削除された回数を指定する。

© 2010 富士通テクノロジー･ソリューションズ

Interface/インターフェイス - インターフェイスにスロット/ポートを指定する。

Transmit Total/合計送信数 - LLDPエージェントが対応するポートで送信したLLDPフレーム数を指定する。

Receive Total/合計受信数 - LLDPエージェントが有効化されている間に、対応するポートでLLDPエージェントが受信した有効なLLDPフレーム数を指定する。

Discards/破棄 - LLDPエージェントが対応するポートでいかなる理由でも破棄したLLDP TLV数を指定する。

Errors/エラー - LLDPエージェントが有効化されている間に、対応するポートでLLDPエージェントが受信した無効なLLDPフレーム数を指定する。

Age outs/エイジアウト - 所与のポートで発生したエイジアウト回数を指定する。 合計エイジアウト数は、特定のMACサービス･アクセス･ポイント (MSAP)により報知された完全な情報セットが、情報タイミング間隔が有効期限を経過したため、遠隔システムと関連付けられたテーブルから削除された回数を指す。

TLV Discards/破棄TLV - LLDPエージェントが対応するポートでいかなる理由でも破棄したLLDP TLV数を指定する。

TLV Unknowns/未知TLV - LLDPエージェントが対応するポートで認識できなかった、ローカル･ポートで受信されたLLDP TLV数を指定する。

コマンドボタン

Refresh/更新 - ページ情報を更新する。

Clear/クリア - すべてのインターフェイスからLLDP統計を消去する。

8.2.10.5 ローカル情報を見る

Information
Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary
Interface: Encl-CB1/0/1
Chassis ID Subtype: MAC Address
Chassis ID: 00:23:8B:17:7B:85
Port ID Subtype: MAC Address
Port ID: 00:23:8B:17:7B:87
System Name:
System Description: FSC PRIMERGY BX900 GbE Connection Blade 36/12, L2+ Switch, Runtime
Port Description:
System Capabilities Supported: bridge
System Capabilities Enabled: bridge
Management Address: 00:23:8B:17:7B:85
Management Address Type: 802
Refresh

図：LLDPローカル情報

選択基準

Interface/インターフェイス - LLDP - 802.1ABフレームを送信できるすべてのポートのリストを指定する。

構成不可能なデータ

Chassis ID Subtype/シャーシIDサブタイプ - シャーシ識別子のソースを説明する文字列を指定する。

Chassis ID/シャーシID - ローカル･システムと関連付けられたシャーシ･コンポーネントを識別するために使用される文字列値を指定する。

Port ID Subtype/ポートIDサブタイプ - ポート識別子のソースを説明する文字列を指定する。

Port ID/ポートID - ポート識別子のソースを説明する文字列を指定する。

System Name/システム名 - ローカル･システムのシステム名を指定する。

System Description/システム内容 - ローカル･システムと関連付けられた選択されたポートの内容を指定する。

Port Description/ポート内容 - ローカル･システムと関連付けられた選択されたポートの内容を指定する。.

System Capabilities Supported/サポートされるシステム機能 - ローカル･システムのシステム機能を指定する。

System Capabilities Enabled/有効化されたシステム機能 - ローカル･システムのサポートされ有効化されたシステム機能を指定する。

Management Address/管理アドレス - ローカル･システムの報知された管理アドレスを指定する。

Management Address Type/管理アドレス･タイプ - 管理アドレスのタイプを指定する。

コマンドボタン

Refresh/更新 - ページ情報を更新する。

8.2.10.6 ローカル･サマリを見る

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Interface	Port ID	Port Description
Encl-CB1/0/1	00:23:8B:17:7B:87	
Encl-CB1/0/2	00:23:8B:17:7B:87	
Encl-CB1/0/3	00:23:8B:17:7B:87	
Encl-CB1/0/4	00:23:8B:17:7B:87	
Encl-CB1/0/5	00:23:8B:17:7B:87	
Encl-CB1/0/6	00:23:8B:17:7B:87	
Encl-CB1/0/7	00:23:8B:17:7B:87	
Encl-CB1/0/8	00:23:8B:17:7B:87	
Encl-CB1/0/9	00:23:8B:17:7B:87	
Encl-CB1/0/10	00:23:8B:17:7B:87	
Encl-CB1/0/11	00:23:8B:17:7B:87	
Encl-CB1/0/12	00:23:8B:17:7B:87	
Encl-CB1/0/13	00:23:8B:17:7B:87	
Encl-CB1/0/14	00:23:8B:17:7B:87	
Encl-CB1/0/15	00:23:8B:17:7B:87	
Encl-CB1/0/16	00:23:8B:17:7B:87	
Encl-CB1/0/17	00:23:8B:17:7B:87	
Encl-CB1/0/18	00:23:8B:17:7B:87	
Encl-CB1/0/19	00:23:8B:17:7B:87	
Encl-CB1/0/20	00:23:8B:17:7B:87	
Encl-CB1/0/21	00:23:8B:17:7B:87	
Encl-CB1/0/22	00:23:8B:17:7B:87	
Encl-CB1/0/23	00:23:8B:17:7B:87	
Encl-CB1/0/24	00:23:8B:17:7B:87	
Encl-CB1/0/25	00:23:8B:17:7B:87	
Encl-CB1/0/26	00:23:8B:17:7B:87	
Encl-CB1/0/27	00:23:8B:17:7B:87	
Encl-CB1/0/28	00:23:8B:17:7B:87	
Encl-CB1/0/29	00:23:8B:17:7B:87	

図：LLDP ローカル･サマリ

構成不可能なデータ

Interface/インターフェイス - LLDP - 802.1ABフレームを送信できるポートを指定する。

Port ID/ポートID - ポート識別子のソースを説明する文字列を指定する。

Port Description/ポート内容 - ローカル･システムと関連付けられたポートの内容を指定する。

© 2010 富士通テクノロジー･ソリューションズ

コマンドボタン

Refresh/更新 - ページ情報を更新する。

8.2.10.7 遠隔情報を見る

図 : LLDP遠隔情報

選択基準

Local Interface/ローカル･インターフェイス - LLDPフレームを受信できるすべてのローカル･ポートをを指定する。

構成不可能なデータ

Chassis ID Subtype/シャーシIDサブタイプ - シャーシ識別子のソースを指定する。

Chassis ID /シャーシID - リモート･システムと関連付けられたシャーシ･コンポーネントを指定する。

Port ID Subtype/ポートIDサブタイプ - ポート識別子のソースを指定する。

Port ID/ポートID - リモート･システムと関連付けられたポート･コンポーネントを指定する。

System Name/システム名 - リモート･システムのシステム名を指定する。

System Description/システム内容 - リモート･システムと関連付けられた所与のポートの内容を指定する。

Port Description/ポート内容 - リモート･システムと関連付けられた所与のポートの内容を指定する。

System Capabilities Supported/サポートされるシステム機能 - リモート･システムのシステム機能を指定する。

System Capabilities Enabled/有効化されたシステム機能 - リモート･システムのサポートされ有効化されたシステム機能を指定する。

Time to Live/TTL - 受信されたリモート･エントリのTTL値を秒数で指定する。

管理アドレス

- **Management Address/管理アドレス** - リモート･システムの通知された管理アドレスを指定する。
- **Type/タイプ** - 管理アドレスのタイプを指定する。

コマンドボタン

更新 - ページ情報を更新する。

8.2.10.8　リモート･サマリを見る

Information

Interface Summary | Statistics | Local Info | Local Summary | Remote Info | Remote Summary

Local Interface	Chassis ID	Port ID	System Name
Encl-CB1/0/48	00:1E:68:85:F5:F1	00:1E:68:85:F5:F3	

Refresh　Clear

図 ：LLDPリモート･サマリ

構成不可能なデータ

Local Interface/ローカル･インターフェイス　リモート･システムにより報知されたLLDPフレームを受信できるローカル･ポートを指定する。

/シャーシID - リモート･システムと関連付けられたシャーシ･コンポーネントを指定する。.

Port ID / ポートID - リモート･システムと関連付けられたポート･コンポーネントを指定する。.

System Name/システム名 - リモート･システムのシステム名を指定する。

コマンドボタン

Refresh/更新 - ページ情報を更新する。

Clear/クリア - すべてのインターフェイスで受信されたLLDPリモートデバイス情報を消去する。

© 2010 富士通テクノロジー･ソリューションズ

8.2.11 DHCPクライアント

8.2.11.1 DHCPクライアント識別子

IBPのDCHPクライアント識別子を指定する。 DHCPクライアント識別子はDHCPサーバとのすべての通信にクライアント識別子を含むために使用される。 識別子タイプはDHCPサーバの要件によって異なる。

> **i** DHCPクライアント識別子はホスト名が変更されると構成で直ちに変更される。 新たなDHCPクライアント識別子を作動させるためには更新操作(再起動または"oob protocol none” と ”oob protocol dhcp"コマンドが必要である。

DHCP Client
DHCP Client-Identifier | DHCP Restart | DHCP6 Restart
Current DHCP Identifier Text: CB.SQ834LW00001
DHCP Identifier: Default
Apply

図： DHCPクライアント識別子

選択基準

DHCP Identifier/DHCP識別子 - DHCP識別子の種類を指定する。

- デフォルト
- 特定の文字列
- 特定の 16 進数値

構成不可能なデータ

Current DHCP Identifier (Hex/Text)(現在のDHCP識別子(hex/文字列) - DHCP識別子の現在の設定を表示する。

構成可能データ

Text String/文字列 - 文の文字列。

Hex Value/16進数値 - 16進数値。

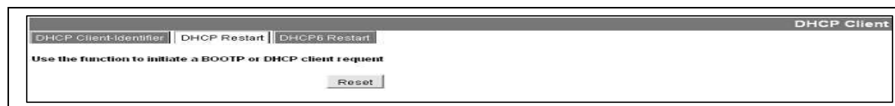
コマンドボタン

Apply - 更新された画面をIBPに送りDHCPクライアント識別子の設定を実行する。

8.2.11.2 DHCP再起動

このコマンドはBOOTPまたはDHCPクライアント要求を、ip addressコマンドによりBOOTPまたはDHCPモードに設定された任意のIPインターフェイスに発行する。 DHCPはサーバがクライアントの最後のアドレスがあるならそれを再割当てするよう要求する。 BOOTPまたはDHCPサーバが別のドメインに移動された場合、クライアントに発行されたアドレスのネットワーク部分は新たなドメインに基づくことになる。

© 2010 富士通テクノロジー・ソリューションズ



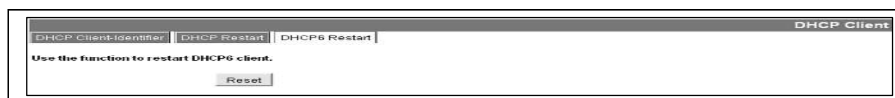
図： DHCP再起動

コマンドボタン

Reset/リセット - 更新された画面をIBPに送りDHCP クライアントの再起動を実行する。

8.2.11.3 DHCP6 再起動

このコマンドはDHCP6クライアント要求を、ip addressコマンドによりDHCPモードに設定された任意のIPインターフェイスに発行する。 DHCPはサーバがクライアントの最後のアドレスがあるならそれを再割当てするよう要求する。 DHCPサーバが別のドメインに移動された場合、クライアントに発行されたアドレスのネットワーク部分は新たなドメインに基づくことになる。



図：DHCP6再起動

コマンドボタン

Reset/リセット -更新された画面をIBPに送りDHCP6クライアントの再起動を実行する。

8.2.12　DNSリレー

8.2.12.1　DNSリレー･コンフィグ

DNSプロトコルはホスト名をIPアドレスにマッピングするための分散データベースであるドメイン･ネーム･システム(DNS)を制御する。 DNSをIBPに構成するとき、ホスト名を ping, telnet, tracerouteおよびTelnetサポート操作等のすべてのIPコマンドによりIPアドレスで代替できる。 ドメイン名を追跡するためIPではドメイン･ネーム･サーバというコンセプトが定義されており、これにはIPアドレスに対応させた名前のキャッシュ (すなわちデータベース) がある。 ドメイン名とIPアドレスを対応させるには、まずホスト名を定義し、ネットワークにあるネームサーバを指定してからDNSを有効化しなければならない。

DNS Relay
DNS Relay Config | Domain Name Config | Name Server Config | DNS Cache Summary | Hosts Config
Admin Mode: Disable
Default Domain Name:
Apply

図 : DNSリレー･コンフィグ

選択基準

Admin Mode/管理モード - プルダウン･メニューから有効化または無効化を選択する。 'enable' (有効化)を選択すると、IPドメイン･ネーミング･システム (DNS)によるホスト名とアドレスの変換が有効化される。

構成可能データ

Default Domain Name/デフォルト･ドメイン名 –

未認定のホスト名を完了させるために使用されるデフォルト･ドメイン名 未認定の名前をドメイン名から分離する初期フェーズは含めないこと。 これは63文字までの文字列である。

コマンドボタン

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。.

変更は保存を実行しなければパワー･サイクル後、保持されない。

8.2.12.2　ドメイン名コンフィグ

不完全なホスト名 (すなわち、ピリオド表記でフォーマットされていないクライアントから渡されたホスト名) に付加できるドメイン名の構成パラメータを変更するためにこの画面は使用できる。 テーブルの内容を表示するためにもこの画面を使用できる。

DNS Relay
DNS Relay Config | Domain Name Config | Name Server Config | DNS Cache Summary | Hosts Config
Domain: Create
Domain Name:*
* = mandatory
Apply | Delete All

図 : DNSリレー･ドメイン名コンフィグ

選択基準

Domain/ドメイン - 追加の"Create".オプション付きで既存のドメイン名をすべて指定する。 "Create"を選択すると別のテキストボックス"Domain Name"が表示され、ここには構成するドメイン名を入力できる。

構成可能データ

Domain Name/ドメイン名 - ドメイン名を指定する。 未認定の名前をドメイン名から分離する初期フェーズは含めないこと。 これは63文字までの文字列である。

コマンドボタン

Apply - 更新された構成をIBPに送る。. 構成変更は直ちに効力を発する。.

Delete/削除 - ドメイン名エントリを削除する。 更新された構成をIBP設定する。 構成変更は直ちに反映される。.

Delete All/全削除 - すべてのドメイン名エントリを削除する。 更新された構成をIBPに送る。. 構成変更は直ちに効力を発する。

8.2.12.3 ネームサーバ・コンフィグ

ドメイン・ネームサーバの構成パラメータを変更するためにこの画面を使用できる。 テーブルの内容を表示するためにもこの画面を使用できる。

図： DNSリレー・ネームサーバ・コンフィグ

選択基準

Name Server/ネームサーバ - 追加の"Create".オプション付きで既存のドメイン・ネームサーバをすべて指定する。 "Create"を選択すると別のテキストボックス"IP Address"が表示され、ここには構成するドメイン・ネームサーバを入力できる。

構成可能データ

IP Address/ IPアドレス - ドメイン・ネームサーバのアドレスを指定する

構成不可能なデータ

Request/要求 - 直前のエージェント再起動以降のDNS要求数を指定する。

Response/応答 - 直前のエージェント再起動以降のDNSサーバ応答数を指定する。

コマンドボタン

Apply - 更新された構成をIBPに送る。. 構成変更は直ちに効力を発する。

Delete - ドメイン・ネームサーバエントリを削除する。更新された構成をIBPに送る。. 構成変更は直ちに効力を発する。.

Delete All/全削除 - すべてのドメイン・ネームサーバ・エントリを削除する。 更新された構成をIBPに送る。. 構成変更は直ちに効力を発する。

© 2010 富士通テクノロジー・ソリューションズ

Clear All Counter/全てのカウンターをクリア - すべてのネームサーバ･カウンターをクリアする。

8.2.12.4 DNSキャッシュ･サマリ

ドメイン･ネーム･システム (DNS)はIPアドレスにドメイン名を動的にマップする。 このパネルはDNSキャッシュの現在の内容を表示する。

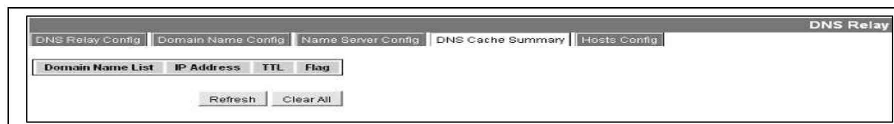


図 : DNSキャッシュ･サマリ

構成不可能なデータ

Domain Name List/ドメイン･ネーム･リスト - このレコードに関連付けられたドメイン･ネーム

IP address/IPアドレス - このレコードに関連付けられたIPアドレス。

TTL - ネームサーバによりリポートされたTimeToLive。

Flag/フラグ - レコードのフラグ。

コマンドボタン

Refresh/更新 - 最新のDNSキャッシュ･エントリにより頁を更新する。

Clear All/全クリア - DNSキャッシュ内すべてのエントリを消去する。

8.2.12.5 ホスト･コンフィグ

DNSテーブルにある静的エントリの構成パラメータを変更するためにこの画面を使用できる。 テーブルの内容を表示するためにもこの画面を使用できる。

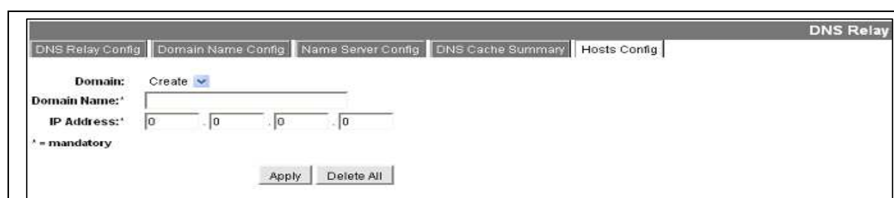


図 : DNSリレー･ホスト･コンフィグ

選択基準

Domain/ドメイン - 追加の"Create".オプション付きで既存のホストをすべて指定する。 "Create"を選択すると別のテキストボックス"Domain Name"が表示され、ここには構成するホストを入力できる。

構成可能データ

Domain Name/ドメイン名 - ホストのドメイン名を指定する。 これは63文字までの文字列である。

IP Address/IP アドレス - ホストのIPアドレスを指定する。

コマンドボタン

Apply - 更新された構成をIBPに送る。. 構成変更は直ちに効力を発する。.

Delete/削除 - ホスト･エントリを削除する。更新された構成をIBPに送る。. 構成変更は直ちに効力を発する。.

Delete All/全削除 - ホストの全エントリを削除する。 更新された構成をIBPに送る。. 構成変更は直ちに効力を発する。.

8.2.13 IPv6

8.2.13.1 統計

IPv6

Statistics

Management Type: In-Band

IPv6 Statistics	
Total Datagrams Received	0
Received Datagrams Locally Delivered	0
Received Datagrams Discarded Due To Header Errors	0
Received Datagrams Discarded Due To MTU	0
Received Datagrams Discarded Due To No Route	0
Received Datagrams With Unknown Protocol	0
Received Datagrams Discarded Due To Invalid Address	0
Received Datagrams Discarded Dut To Truncated Data	0
Received Datagrams Discarded Other	0
Received Datagrams Reassembly Required	0
Datagrams Successfully Reassembled	0
Datagrams Failed To Reassemble	0
Datagrams Forwarded	0
Datagrams Locally Trasmitted	2
Datagrams Transmit Failed	0
Datagrams Successfully Fragmented	0
Datagrams Failed To Fragment	0
Datagrams Fragments Created	0
Multicast Datagrams Received	0
Multicast Datagrams Transmitted	2
ICMPv6 Statistics	
Total ICMPv6 Messages Received	0
ICMPv6 Messages With Errors Received	0
ICMPv6 Destination Unreachable Messages Received	0
ICMPv6 Messages Prohibited Administratively Received	0

図： IPv6 統計

選択基準

Management Type/管理タイプ - 構成すべきポート･タイプを指定する。 この選択が変更されると、画面が更新されてすべての欄は新たに選択されたポート･タイプに更新される。

構成不可能なデータ

IPv6 統計

Total Datagrams Received/データグラム受信総数 - インターフェイスにより受信された入力データグラムの総数、エラー有りで受信されたものを含む。

Received Datagrams Locally Delivered/ローカルでデリバリされた受信データグラム - IPv6ユーザー･プロトコル (ICMPを含む) にデリバリが完了したデータグラム合計数。 このカウンターはデータグラム

の一部のための入力インターフェイスではないことがある当該データグラムが宛てられたインターフェイスで1ずつ増加される。

Received Datagrams Discarded Due To Header Errors/ヘッダー・エラーにより破棄された受信データグラム - バージョン不一致、他のフォーマット・エラー、ホップ数の超過、IPv6の処理中に発見されたエラー等を含むIPv6ヘッダーにあるエラーが原因で破棄された入力データグラム数。

Received Datagrams Discarded Due To MTU/MTUが原因で破棄された受信データグラム - 入力データグラムのうちそのサイズがアウトバウンド・インターフェイスのリンクMTUを超過したために転送できなかった入力データグラム数。

Received Datagrams Discarded Due To No Route/ルートが無いため破棄された受信データグラム - ターゲットに送信するためのルートが見つからなかったために破棄された入力データグラム数。

Received Datagrams With Unknown Protocol/プロトコル不明な受信データグラム - 受信には成功したがプロトコルが不明またはサポートされないため破棄されたローカルに宛てられたデータグラム数。このカウンターはデータグラムの一部のための入力インターフェイスではないことがある当該データグラムが宛てられたインターフェイスで1ずつ増加される。

Received Datagrams Discarded Due To Invalid Address/無効アドレスにより破棄された受信データグラム - IPv6ヘッダーのターゲット欄にあるIPv6アドレスがこのエンティティで受信されたが、有効なアドレスではなかったために破棄された入力データグラム数。 この計数には無効アドレスやサポートされないアドレス(たとえば、未割当てのプレフィックス付きアドレス) を含む。 IPv6ルーターではないためデータグラムを転送しないエンティティについては、このカウンターはターゲット・アドレスがローカル・アドレスでなかったために破棄されたデータグラムを含む。

Received Datagrams Discarded Dut To Truncated Data/データ中断により破棄された受信データグラム - データグラム・フレームに十分なデータがないために破棄された入力データグラム数。

Received Datagrams Discarded Other/他の理由で破棄された受信データグラム - 処理継続を中断すべき問題がないにもかかわらず破棄された(たとえば、バッファー・スペースの欠如等) 入力IPv6データグラム数。 このカウンターが再アセンブリを待機中に破棄されたデータグラムを含まないことに注意する。

Received Datagrams Reassembly Required/再アセンブリを要する受信データグラム - このインターフェイスで再アセンブリを要する受信IPv6フラグメント数。 このカウンターはフラグメントの一部のための入力インターフェイスではないことがある当該フラグメントが宛てられたインターフェイスで1ずつ増加される。

Datagrams Successfully Reassembled/再アセンブリが成功したデータグラム - IPv6再アセンブリが成功したデータグラム数。 このカウンターはフラグメントの一部のための入力インターフェイスではないことがある当該データグラムが宛てられたインターフェイスで1ずつ増加される。

Datagrams Failed To Reassemble/再アセンブリに失敗したデータグラム - (タイムアウトやエラー等なんらかの理由で) IPv6再アセンブリ・アルゴリズムにより検出 された障害数。 一部のアルゴリズム(特にRFC815のアルゴリズム)はフラグメントを受信されると結合させることによりフラグメント数を追跡できなくなるため、この値は破棄されたIPv6フラグメントでは必ずしもないことに注意する。 このカウンターはフラグメントの一部のための入力インターフェイスではないことがある当該フラグメントが宛てられたインターフェイスで1ずつ増加される。

Datagrams Forwarded/転送されたデータグラム - このエンティティが受信し最終ターゲットに転送した出力データグラム数。 IPv6ルーターとしては機能しないエンティティの場合、このカウンターhこのエンティティを通してソース・ルートされ、ソース・ルート処理に成功したパケットのみを含む。 転送が成功したデータグラムについてアウトバウンド・インターフェイスのカウンターはインクリメントされる。

Datagrams Locally Transmitted/ローカルで送信されたデータグラム - この出力インターフェイスからこのエンティティが送信に成功したデータグラム数。

Datagrams Transmit Failed/送信失敗データグラム - このエンティティが送信に失敗したデータグラム数。

Datagrams Successfully Fragmented/フラグメント化に成功したデータグラム - この出力インターフェイスでフラグメント化に成功したIPv6データグラム数。

Datagrams Failed To Fragment/フラグメント化に失敗したデータグラム - この出力インターフェイスでフラグメント化に失敗したIPv6データグラム数。

Datagrams Fragments Created/生成されたデータグラム・フラグメント - この出力インターフェイスでフラグメント化の結果生成された出力データグラム・フラグメント数

Multicast Datagrams Received/受信されたマルチキャスト・データグラム - インターフェイスに受信されたマルチキャスト・パケット数。

Multicast Datagrams Transmitted/送信されたマルチキャスト・データグラム - インターフェイスにより送信されたマルチキャスト・パケット数。

© 2010 富士通テクノロジー・ソリューションズ

ICMPv6 統計

Total ICMPv6 Messages Received/ICMPv6受信メッセージ総数 - ipv6IfIcmpInErrorsコマンドにより計数されたものをすべて含むICMPメッセージの合計数。 このインターフェイスはメッセージのための入力インターフェイスではないことがある当該ICMPメッセージが宛てられたインターフェイスであることに注意する。

ICMPv6 Messages With Errors Received/エラー有りで受信されたICMPｖ6メッセージ - インターフェイスが受信したがICMP固有エラー(間違ったICMPチェックサム、間違った長さ等)があると判断されたICMPメッセージ数。

ICMPv6 Destination Unreachable Messages Received/受信されたICMPｖ6ターゲット未到達メッセージ - インターフェイスが受信したICMPｖ6ターゲット未到達メッセージ数。

ICMPv6 Messages Prohibited Administratively Received/受信されたが管理上禁止されたICMPｖ6メッセージ - インターフェイスが受信したICMPｖ6ターゲット未到達で通信管理上禁止されたメッセージ数。

ICMPv6 Time Exceeded Messages Received/受信されたICMPｖ6時間超過メッセージ - インターフェイスが受信したICMPｖ6時間超過メッセージ数。

ICMPv6 Parameter Problem Messages Received/受信されたICMPｖ6パラメータ障害有りのメッセージ - インターフェイスが受信したICMPｖ6パラメータ障害有りのメッセージ数。

ICMPv6 Packet Too Big Messages Received/受信されたICMPｖ6過大パケットサイズメッセージ - インターフェイスが受信したICMPｖ6過大パケットサイズメッセージ数。

ICMPv6 Echo Request Messages Received/受信されたICMPｖ6エコー要求メッセージ - インターフェイスが受信したICMPｖ6エコー要求メッセージ数。

ICMPv6 Echo Reply Messages Received/受信されたICMPｖ6エコー応答メッセージ - インターフェイスが受信したICMPｖ6エコー応答メッセージ数。

ICMPv6 Router Solicit Messages Received/受信されたICMPｖ6ルーター要請メッセージ - インターフェイスが受信したICMPｖ6ルーター要請メッセージ数。

ICMPv6 Router Advertisement Messages Received/受信されたICMPｖ6ルーター通知メッセージ - インターフェイスが受信したICMPｖ6ルーター通知メッセージ数。

ICMPv6 Neighbor Solicit Messages Received/受信されたICMPｖ6近隣要請メッセージ - インターフェイスが受信したICMPｖ6近隣要請メッセージ数。

ICMPv6 Neighbor Advertisement Messages Received/受信されたICMPｖ6近隣通知メッセージ - インターフェイスが受信したICMPｖ6近隣通知メッセージ数。

ICMPv6 Redirect Messages Received/受信されたICMPv6リダイレクト･メッセージ - インターフェイスが受信したICMPｖ6リダイレクト･メッセージ数。

ICMPv6 Group Membership Query Messages Received/受信されたICMPv6グループ･メンバーシップ･クエリー･メッセージ - インターフェイスが受信したICMPｖ6グループ･メンバーシップ･クエリー･メッセージ数。

ICMPv6 Group Membership Response Messages Received/受信されたICMPv6グループ･メンバーシップ応答メッセージ - インターフェイスが受信したICMPｖ6グループ･メンバーシップ応答メッセージ数。

ICMPv6 Group Membership Reduction Messages Received/受信されたICMPv6グループ･メンバーシップ削除メッセージ - インターフェイスが受信したICMPｖ6グループ･メンバーシップ削メッセージ数。

Total ICMPv6 Messages Transmitted/送信されたICMPｖ6メッセージ合計数 - このインターフェイスが送信を試行したICMPメッセージ総数。 このカウンターはすべてのicmpOutErrorsコマンドが計数したものを含むことに注意する。

ICMPv6 Messages Not Transmitted Due To Error/エラーにより送信されなかったICMPｖ6メッセージ - バッファー欠如等のICMP内で発見された障害によりこのインターフェイスが送信しなかったICMPメッセージ数。 この値にはIPｖ6が結果データグラムをルートできないこと等のICMPレイヤー外で発見されたエラーは含まない。 実装によってはこのカウンターの値に影響しないタイプのエラーがあることがある。

© 2010 富士通テクノロジー･ソリューションズ

ICMPv6 Destination Unreachable Messages Transmitted/送信されたICMPｖ6ターゲット到達不可メッセージ - インターフェイスが送信したICMPｖ6ターゲット到達不可メッセージ数。

ICMPv6 Messages Prohibited Administratively Transmitted/送信されたが管理上禁止されたICMPv6メッセージ - 送信されたがICMPターゲット到達不可や通信管理上禁止されたメッセージ数。

ICMPv6 Time Exceeded Messages Transmitted/送信されたICMPｖ6時間超過メッセージ - インターフェイスが送信したICMPｖ6時間超過メッセージ数。

ICMPv6 Parameter Problem Messages Received/受信されたICMPｖ6パラメータ障害有りのメッセージ - インターフェイスが送信したICMPｖ6パラメータ障害有りのメッセージ数。

ICMPv6 Packet Too Big Messages Transmitted/送信されたICMPｖ6過大パケットサイズメッセージ - インターフェイスが送信したICMPｖ6過大パケットサイズメッセージ数。

ICMPv6 Echo Request Messages Transmitted/送信されたICMPｖ6エコー要求メッセージ - インターフェイスが送信したICMPｖ6エコー(要求)メッセージ数。

ICMPv6 Echo Reply Messages Transmitted/送信されたICMPｖ6エコー応答メッセージ - インターフェイスが送信したICMPエコー応答メッセージ数。

ICMPv6 Router Solicit Messages Transmitted/送信されたICMPｖ6ルーター要請メッセージ - インターフェイスが送信したICMP近隣要請メッセージ数。

ICMPv6 Router Advertisement Messages Transmitted/送信されたICMPｖ6ルーター通知メッセージ - インターフェイスが送信したICMPルーター通知メッセージ数。

ICMPv6 Neighbor Solicit Messages Transmitted/送信されたICMPｖ6近隣要請メッセージ - インターフェイスが送信したICMP近隣要請メッセージ数。

ICMPv6 Neighbor Advertisement Messages Transmitted/送信されたICMPｖ6近隣通知メッセージ - インターフェイスが送信したICMP近隣通知メッセージ数。

ICMPv6 Redirect Messages Transmitted/送信されたICMPv6リダイレクト･メッセージ - 送信されたICMPv6リダイレクト･メッセージ数。

ICMPv6 Group Membership Query Messages Transmitted/送信されたICMPv6グループ･メンバーシップ･クエリー･メッセージ - 送信されたICMPｖ6グループ･メンバーシップ･クエリー･メッセージ数。

ICMPv6 Group Membership Response Messages Transmitted/送信されたICMPv6グループ･メンバーシップ応答メッセージ - 送信されたICMPｖ6グループ･メンバーシップ応答メッセージ数。

ICMPv6 Group Membership Reduction Messages Transmitted/送信されたICMPv6グループ･メンバーシップ削除メッセージ - 送信されたICMPｖ6グループ･メンバーシップ削除メッセージ数。

ICMPv6 Duplicate Address Detects/ICMPv6重複アドレス検出数 - インターフェイスが検出した重複アドレス数

コマンドボタン

Clear/クリア - IPv6統計を消去する。

Refresh/更新 - 画面を最新データで更新する。

© 2010 富士通テクノロジー･ソリューションズ

8.3　　グループ管理メニュー

この節は、アップリンクセット、ポート･グループ、VLANポート･グループ、サービスLAN、サービスVLAN、ポート、ポート･チャネル、ポート･バックアップの構成方法を説明する。

8.3.1　　グループ･リスト

8.3.1.1　　サマリ

この頁にはすべての現在構成されたポート･グループのサマリを表示する。

Group List

Summary

Page			1		
Unit/Slot/Port	Uplink Sets	Port Groups	VLAN Port Groups	Service LAN	Service VLAN
Encl-CB1/0/1		default			
Encl-CB1/0/2		default			
Encl-CB1/0/3		default			
Encl-CB1/0/4		default			
Encl-CB1/0/5		default			
Encl-CB1/0/6		default			
Encl-CB1/0/7		default			
Encl-CB1/0/8		default			
Encl-CB1/0/9		default			
Encl-CB1/0/10		default			
Encl-CB1/0/11		default			
Encl-CB1/0/12		default			
Encl-CB1/0/13		default			
Encl-CB1/0/14		default			
Encl-CB1/0/15		default			
Encl-CB1/0/16		default			
Encl-CB1/0/17		default			
Encl-CB1/0/18		default			
Encl-CB1/0/19		default			
Encl-CB1/0/20		default			
Encl-CB1/0/21		default			
Encl-CB1/0/22		default			
Encl-CB1/0/23		default			
Encl-CB1/0/24		default			

図 ： グループ･リスト･サマリ

構成不可能なデータ

Slot/Port | スロット/ポート - ポートを識別する。

Uplink Sets/アップリンク･セット - アップリンク･セットのグループ名。

Port Groups/ポート･グループ - ポート･グループの名前。

VLAN Port Groups/VLANポート･グループ - VLANポート･グループの名前。

Service LAN/サービスLAN - サービスLANのグループ名。

Service LAN/サービスVLAN - 　サービスLANのグループ名。

コマンドボタン

Refresh/更新- 構成値を再度取得する。

© 2010 富士通テクノロジー・ソリューションズ

8.3.2 アップリンク・セット

「アップリンク・セット」は、サーバ・グレード・グループを業務LANへ接続するためにポート・グループ定義で使用される1からnの外部（アップリンク）ポートの集合として定義される。 アップリンク・セットの構成目的はグループの生成、既存外部ポートのグループへの追加または変更である。 この頁ではリンク・ステート、ポート・バックアップ、アップリンク・セット・グループのIGMPスヌーピングを構成できる。

8.3.2.1 コンフィグ

Uplink Sets

Config | Status

Uplink Set Name: default
Uplink Set Name:* default
Link State: Enable
Port Backup: Disable
IGMP Snooping: Enable
LACP: Disable

Page		1	
Unit/Slot/Port	Type	Status	Participation
Encl-CB1/0/37	External	Exclude	Exclude
Encl-CB1/0/38	External	Exclude	Exclude
Encl-CB1/0/39	External	Include	Include
Encl-CB1/0/40	External	Include	Include
Encl-CB1/0/41	External	Include	Include
Encl-CB1/0/42	External	Include	Include
Encl-CB1/0/43	External	Include	Include
Encl-CB1/0/44	External	Include	Include
Encl-CB1/0/45	External	Include	Include
Encl-CB1/0/46	External	Include	Include

* = mandatory

Apply

図 :アップリンク・セット・コンフィグ:

選択基準

Uplink Set Name / アップリンク・セット名 - このプルダウン・メニューで既存アップリンク・セットから1個を選択する。

Link State/リンク・ステート - このプルダウン・メニューでリンク・ステートを構成する。

Port Backup/ポート・バックアップ - このプルダウン・メニューでポート・バックアップを構成する。

IGMP Snooping/IGMPスヌーピング - このプルダウン・メニューでIGMPスヌーピングを構成する。

LACP - このプルダウン・メニューでLACPを構成する。

Participation/参加 - この欄を使用してインターフェイスがこのアップリンク・セットに参加するかを指定する。 工場側デフォルトは'Exclude'（参加させない）である。 とりうる値:

– Include（含める）- このインターフェイスはこのアップリンク・セットに参加する。

– Exclude（除く）- このインターフェイスはこのアップリンク・セットに参加しない。

構成可能データ

Uplink Set Name/アップリンク・セット名 - アップリンク・セット名を入力して新グループを生成する。

© 2010 富士通テクノロジー・ソリューションズ

構成不可能なデータ

Slot/Port / スロット/ポート - 当該インターフェイス。

Type / タイプ -インターフェイスの種類。 この種類は外部とする。

Status/ステータス - インターフェイスがこのアップリンク･セットに属するか否かを示す。

コマンドボタン

Apply - IBP を画面の値で更新する。IBPにパワー･サイクル後、設定を保持させるには、保存を実行しなければならない。. .。. .

Delete/削除 -アップリンク･セットを削除する。 デフォルト･アップリンク･セットは削除できない。

8.3.2.2 ｽﾃｰﾀｽ

この頁は現在構成されたすべてのアップリンク･セットを表示する。

Uplink Sets

Config | Status

Uplink Set Name	External Active Ports			External Backup Ports		Link State	Port Backup	IGMP Snoopin
default	Logical Interface	Encl-CB1/1/1				Enable	Disable	Enable
	Encl-CB1/0/39	Encl-CB1/0/40	Encl-CB1/0/41	Logical Interface	Encl-CB1/1/2			
	Encl-CB1/0/42	Encl-CB1/0/43	Encl-CB1/0/44					
	Encl-CB1/0/45	Encl-CB1/0/46						

図 : アップリンク･セット･ステータス

構成不可能なデータ

Uplink Set Name/アップリンク･セット名 -アップリンク･セット名。

External Active Ports/アクティブな外部ポート - アクティブな外部ポート･メンバーをリストする。

External Backup Ports/外部バックアップ･ポート - 外部バックアップ･ポートをリストする。

Logical Interface/論理インターフェイス - 論理インターフェイスをリストする。

Link State/リンク･ステート - リンク･ステートのステータス。

Port Backup/ポート･バックアップ - バックアップの状態。

IGMP Snooping/IGMPスヌーピング - IGMPスヌーピングの状態。

LACP - LACPの状態。

© 2010 富士通テクノロジー･ソリューションズ

8.3.3　　ポート･グループ

ポート･グループ構成の目的はポート･グループの生成および既存ポート･グループの変更である。 内部ポートのみポート･グループのメンバーに定義できる。 外部接続はアップリンク･セットを指定して定義される。

8.3.3.1　　コンフィグ

Port Groups

Config | Status

Group Name: default
Group Name:* default
Uplink Set Name: default

Page		1	
Unit/Slot/Port	Type	Status	Participation
Encl-CB1/0/1	Internal	Include	Include
Encl-CB1/0/2	Internal	Include	Include
Encl-CB1/0/3	Internal	Include	Include
Encl-CB1/0/4	Internal	Include	Include
Encl-CB1/0/5	Internal	Include	Include
Encl-CB1/0/6	Internal	Include	Include
Encl-CB1/0/7	Internal	Include	Include
Encl-CB1/0/8	Internal	Include	Include
Encl-CB1/0/9	Internal	Include	Include
Encl-CB1/0/10	Internal	Include	Include
Encl-CB1/0/11	Internal	Include	Include
Encl-CB1/0/12	Internal	Include	Include
Encl-CB1/0/13	Internal	Include	Include
Encl-CB1/0/14	Internal	Include	Include
Encl-CB1/0/15	Internal	Include	Include
Encl-CB1/0/16	Internal	Include	Include
Encl-CB1/0/17	Internal	Include	Include
Encl-CB1/0/18	Internal	Include	Include
Encl-CB1/0/19	Internal	Include	Include
Encl-CB1/0/20	Internal	Include	Include

図 ： ポート･グループ･コンフィグ

選択基準

Group Name/グループ名 - このプルダウン･メニューで既存グループから1個を選択する。

Uplink Set Name/アップリンク･セット名 - このプルダウン･メニューで外部接続を指定する。 プルダウン･メニューに"----------"が出れば、利用できるアップリンク･セットは無い。

Participation/参加 - この欄を使用してインターフェイスがこのポート･グループに参加するかを指定する。 工場側デフォルトは'Exclude' (参加させない) である。 とりうる値：

– Include (含める) - このインターフェイスはこのポート･グループに参加する。

– Exclude (含める) - このインターフェイスはこのポート･グループに参加しない。

構成可能データ

Group Name/グループ名 - /グループ名を入力して新ポート･グループを生成する。

構成不可能なデータ

Slot/Port / スロット/ポート- ポートを識別する。

Type / タイプ - インターフェイスの種類。 この種類は内部とする。

Status / ｽﾃｰﾀｽ - インターフェイスがこのポート･グループに属するか否かを示す。

コマンドボタン

Apply - IBP を画面の値で更新する。IBPにパワー･サイクル後、設定を保持させるには、保存を実行しなければならない。. .。. .

Delete/削除 - ポート･グループを削除する。 デフォルト･ポート･グループは削除できない。

8.3.3.2 ｽﾃｰﾀｽ

この頁は現在構成されたすべてのポート･グループの状態を表示する。

Port Groups

Config | Status

Port Group Name	Internal Ports			Uplink Set Name	External Ports		
default	Encl-CB1/0/1	Encl-CB1/0/2	Encl-CB1/0/3	default			
	Encl-CB1/0/4	Encl-CB1/0/5	Encl-CB1/0/6				
	Encl-CB1/0/7	Encl-CB1/0/8	Encl-CB1/0/9				
	Encl-CB1/0/10	Encl-CB1/0/11	Encl-CB1/0/12				
	Encl-CB1/0/13	Encl-CB1/0/14	Encl-CB1/0/15		Encl-CB1/0/39	Encl-CB1/0/40	Encl-CB1/0/41
	Encl-CB1/0/16	Encl-CB1/0/17	Encl-CB1/0/18		Encl-CB1/0/42	Encl-CB1/0/43	Encl-CB1/0/44
	Encl-CB1/0/19	Encl-CB1/0/20	Encl-CB1/0/21		Encl-CB1/0/45	Encl-CB1/0/46	
	Encl-CB1/0/22	Encl-CB1/0/23	Encl-CB1/0/24				
	Encl-CB1/0/25	Encl-CB1/0/26	Encl-CB1/0/27				
	Encl-CB1/0/28	Encl-CB1/0/29	Encl-CB1/0/30				
	Encl-CB1/0/31	Encl-CB1/0/32	Encl-CB1/0/33				
	Encl-CB1/0/34	Encl-CB1/0/35	Encl-CB1/0/36				

図 :ポート･グループ･ステータス

構成不可能なデータ

Port Group Name/ポート･グループ名 - ポート･グループの名前。

Internal Ports/内部ポート - 内部ポート･メンバーをリストする。

Uplink Set Name/アップリンク･セット名 - アップリンク･セット名。

External Ports /外部ポート - ポート･グループの外部ポートをリストする。

8.3.4 VLANポート･グループ

8.3.4.1 コンフィグ

VLAN Port Groups

Config | Status

VLAN Port Group Name: Create

VLAN Port Group Name:*

VLAN ID (1 to 4094):* 1

Uplink Set Name:* ----------

Native VLAN: Disable

Page		1	
Unit/Slot/Port	Type	Status	Participation
Encl-CB1/0/1	Internal		Exclude
Encl-CB1/0/2	Internal		Exclude
Encl-CB1/0/3	Internal		Exclude
Encl-CB1/0/4	Internal		Exclude
Encl-CB1/0/5	Internal		Exclude
Encl-CB1/0/6	Internal		Exclude
Encl-CB1/0/7	Internal		Exclude
Encl-CB1/0/8	Internal		Exclude
Encl-CB1/0/9	Internal		Exclude
Encl-CB1/0/10	Internal		Exclude
Encl-CB1/0/11	Internal		Exclude
Encl-CB1/0/12	Internal		Exclude
Encl-CB1/0/13	Internal		Exclude
Encl-CB1/0/14	Internal		Exclude
Encl-CB1/0/15	Internal		Exclude
Encl-CB1/0/16	Internal		Exclude
Encl-CB1/0/17	Internal		Exclude
Encl-CB1/0/18	Internal		Exclude

図 ：VLANポート･グループ･コンフィグ

選択基準

VLAN Port Group Name/VLANポート･グループ名 - 既存VLANポート･グループを構成する、または新たなVLANポート･グループを生成するにはこの画面を使用できる。 このプルダウン･メニューから既存VLANポート･グループから1個を選択する、または'Create'を選択して新たなVLANポート･グループを追加できる。

Uplink Set Name/アップリンク･セット名 - 外部接続用にアップリンク･セットを指定する。 プルダウン･メニューに"----------"が出れば、利用できるアップリンク･セットは無い。

Native VLAN/ネイティブVLAN - 外部インターフェイスの動作を変更する: タグ無しパケットのみ処理し転送する。

- Enable/有効化- このグループの外部インターフェイスはタグ無しパケットのみ処理し転送する。
- Disnable/無効化- このグループの外部インターフェイスはタグ付きとタグ無しのパケットを処理し転送する。

Participation/参加 -この欄を使用してインターフェイスがこのVLANポート･グループに参加するかを指定する。 工場側デフォルトは’Exclude' (参加させない) である。とりうる値:

- Include (含める) - このインターフェイスはこのVLANポート･グループに参加する。
- Exclude (含める) - このインターフェイスはこのVLANポート･グループに参加しない。

構成可能データ

VLAN Port Group Name/VLANポート･グループ名 - 新たなVLANポート･グループに名前をつける。

VLAN ID - VLANポート･グループのVLAN識別子を指定する。 VLAN ID の範囲は1から4094である。

構成不可能なデータ

Slot/Port | スロット - 当該インターフェイス。

Type / タイプ - インターフェイスの種類。 この種類は内部とする。

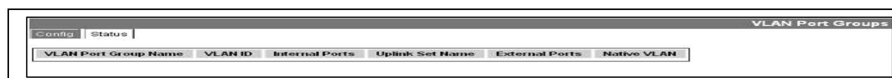
Status / ｽﾃｰﾀｽ - インターフェイスの参加パラメータ現在値を示す。

コマンドボタン

Apply - IBP を画面の値で更新する。IBPにパワー･サイクル後、設定を保持させるには、保存を実行しなければならない

Delete/削除 - VLANポート･グループを削除する。

8.3.4.2 ｽﾃｰﾀｽ



図： 削除ポート･グループ･ステータス

この頁は現在構成されたすべての削除ポート･グループの状態を表示する。

構成不可能なデータ

VLAN Port Group Name/VLANポート･グループ名 - VLANポート･グループの名前。

VLAN ID - VLANポート･グループのVLAN識別子。 VLAN ID の範囲は1から4094である。

Internal Ports/内部ポート - VLANポート･グループのメンバーである内部インターフェイス。

Uplink Set Name/アップリンク･セット名 - アップリンク･セット名を入力して新グループを生成する。

外部ポート - 指定されたアップリンク･セットのメンバーである外部インターフェイス。

Native VLAN/ネイティブVLAN - 外部インターフェイスの動作を変更する: タグ無しパケットのみ処理し転送する。

© 2010 富士通テクノロジー･ソリューションズ

8.3.5 サービスLAN

8.3.5.1 コンフィグ

Service LAN

Config | Status

Service LAN Name: Create
Service LAN Name:*
Service VLAN ID (1 to 4094) :* 1
Uplink Set Name:* ----------

Page		1	
Unit/Slot/Port	Type	Status	Participation
Encl-CB1/0/1	Internal		Exclude
Encl-CB1/0/2	Internal		Exclude
Encl-CB1/0/3	Internal		Exclude
Encl-CB1/0/4	Internal		Exclude
Encl-CB1/0/5	Internal		Exclude
Encl-CB1/0/6	Internal		Exclude
Encl-CB1/0/7	Internal		Exclude
Encl-CB1/0/8	Internal		Exclude
Encl-CB1/0/9	Internal		Exclude
Encl-CB1/0/10	Internal		Exclude
Encl-CB1/0/11	Internal		Exclude
Encl-CB1/0/12	Internal		Exclude
Encl-CB1/0/13	Internal		Exclude
Encl-CB1/0/14	Internal		Exclude
Encl-CB1/0/15	Internal		Exclude
Encl-CB1/0/16	Internal		Exclude
Encl-CB1/0/17	Internal		Exclude
Encl-CB1/0/18	Internal		Exclude
Encl-CB1/0/19	Internal		Exclude

図： サービスLANコンフィグ

選択基準

Service LAN Name/サービスLAN名 - 既存サービスLANを構成する、または新たなサービスLANを生成するにはこの画面を使用できる。 このプルダウン･メニューから既存サービスLANを選択する、または'Create'を選択して新たなサービスLANを追加できる。

Uplink Set Name/アップリンク･セット名 -アップリンク･セット名を入力して新グループを生成する。 . プルダウン･メニューに”----------”が出れば、利用できるアップリンク･セットは無い。

Participation/参加 - この欄を使用してインターフェイスがこのサービスLANに参加するかを指定する。工場側デフォルトは’Exclude' (参加させない) である。 とりうる値：

– Include (含める) - このインターフェイスはこのサービスLANに参加する。
– Exclude (含める) - このインターフェイスはこのサービスLANに参加しない。

構成可能データ

Service LAN Name/サービスLAN名 - 新サービスLANに名前をつける。

Service VLAN ID/サービスVLAN ID - サービスLANのVLAN識別子を指定する。 VLAN ID の範囲は1から4094である。

構成不可能なデータ

Slot/Port - ポートを識別する。

Type / タイプ - インターフェイスの種類。 この種類は内部とする。

Status / ｽﾃｰﾀｽ - インターフェイスの参加パラメータ現在値を示す。

コマンドボタン

Apply - IBP を画面の値で更新する。IBPにパワー･サイクル後、設定を保持させるには、保存を実行しなければならない。

Delete/削除 - サービスLANを削除する。

8.3.5.2 ｽﾃｰﾀｽ

Service LAN

Config | Status

Service LAN Name	Service VLAN ID	Internal Ports	Uplink Set Name	External Ports

図： サービスLANステータス

この頁は現在構成されたすべてのサービスLANを表示する。

構成不可能なデータ

Service LAN Name/サービスLAN名 - サービスLANの名前。

Service VLAN ID/サービスVLAN ID - サービスLANのVLAN識別子。 VLAN ID の範囲は1から4094である。

Internal Ports/内部ポート -サービスLANのメンバーである内部インターフェイス。

Uplink Set Name - アップリンク･セット名を入力して新グループを生成する。

External Ports /外部ポート - 指定されたアップリンク･セットのメンバーである外部インターフェイス。

8.3.6 サービスVLAN

8.3.6.1 コンフィグ

Service VLAN

Config | Status

Service VLAN Name: Create

Service VLAN Name:*

Service VLAN ID (1 to 4094) :* 1

Uplink Set Name:* default

Page		1	
Unit/Slot/Port	Type	Status	Participation
Encl-CB1/0/1	Internal		Exclude
Encl-CB1/0/2	Internal		Exclude
Encl-CB1/0/3	Internal		Exclude
Encl-CB1/0/4	Internal		Exclude
Encl-CB1/0/5	Internal		Exclude
Encl-CB1/0/6	Internal		Exclude
Encl-CB1/0/7	Internal		Exclude
Encl-CB1/0/8	Internal		Exclude
Encl-CB1/0/9	Internal		Exclude
Encl-CB1/0/10	Internal		Exclude
Encl-CB1/0/11	Internal		Exclude
Encl-CB1/0/12	Internal		Exclude
Encl-CB1/0/13	Internal		Exclude
Encl-CB1/0/14	Internal		Exclude
Encl-CB1/0/15	Internal		Exclude
Encl-CB1/0/16	Internal		Exclude
Encl-CB1/0/17	Internal		Exclude
Encl-CB1/0/18	Internal		Exclude
Encl-CB1/0/19	Internal		Exclude

図 ： サービスVLANコンフィグ

選択基準

Service VLAN Name / サービスVLAN名-既存サービスVLANを構成する、または新たなサービスVLANを生成するにはこの画面を使用できる。 このプルダウン･メニューから既存サービスLANを選択する、または'Create'を選択して新たなサービスVLANを追加できる。

Uplink Set Name/アップリンク･セット名-アップリンク･セット名を入力して新グループを生成する。 . プルダウン･メニューに"----------"が出れば、利用できるアップリンク･セットは無い。

Participation/参加 -この欄を使用してインターフェイスがこのサービスVLANに参加するかを指定する。工場側デフォルトは'Exclude' (参加させない) である。 とりうる値：

– Include (含める) - このインターフェイスはこのサービスVLANに参加する。

– Exclude (含める)- このインターフェイスはこのサービスLANに参加しない。

構成可能データ

Service VLAN Name /サービスVLAN名-新サービスVLANに名前をつける。

Service VLAN ID / サービスVLAN ID - サービスVLANのVLAN識別子を指定する。 VLAN ID の範囲は1から4094である。

構成不可能なデータ

Slot/Port - ポートを識別する。

© 2010 富士通テクノロジー･ソリューションズ

Type / タイプ　 - インターフェイスの種類。 この種類は内部とする。

Status / ｽﾃｰﾀｽ - インターフェイスの参加パラメータ現在値を示す。

コマンドボタン

Apply - IBP を画面の値で更新する。IBPにパワー･サイクル後、設定を保持させるには、保存を実行しなければならない。

Delete/削除 - サービスVLANを削除する。

8.3.6.2 ｽﾃｰﾀｽ

Service VLAN

Config | Status

Service VLAN Name	Service VLAN ID	Internal Ports	Uplink Set Name	External Ports

図： サービスVLANステータス

この頁は現在構成されたすべてのサービスVLANを表示する。

構成不可能なデータ

Service LAN Name/サービスLAN名 - サービスVLANの名前。

Service VLAN ID/サービスVLAN ID - サービスVLANのVLAN識別子。 VLAN ID の範囲は1から4094である

Internal Ports/内部ポート - サービスVLANのメンバーである内部インターフェイス。

Uplink Set Name/アップリンク･セット名 –
アップリンク･セット名を入力して新グループを生成する。 .
外部ポート - 指定されたアップリンク･セットのメンバーである外部インターフェイス。.

8.3.7 ポート

8.3.7.1 構成

Port

Config | Summary | Mirroring

Unit/Slot/Port: All
Port Type:
Admin Mode: Enable
E-Keying Status:
Physical Mode:
Physical Status:
Link Status:
Link Trap: Enable
Maximum Frame Size (1518 to 9216) :* 1518
ifIndex:
Flow Control: Disable
Capability: 10 Mbps Full Duplex / 100 Mbps Full Duplex / 1000 Mbps Full Duplex

* = mandatory

Apply

図： ポート･コンフィグ

選択基準

Slot/Port / スロット/ポート - データが表示されるまたは構成されるインターフェイスを選択する.

Admin Mode/管理モード - プルダウン･メニューでポート制御管理ステートを選択する。 ポートをネットワークに参加させるには'enable'(有効化する)を選択する。 デフォルト設定は有効化されている。

Physical Mode/物理モード - プルダウン･メニューでポートの速度と二重モードを選択する。 Auto (オート) を選択すると、二重モードと速度が自動ネゴシエーションにより設定される。 ポートの最高性能 (全二重で100Mbps)が通知されることに注意する。 その他のポートの二重モードと転送速度は選択できる。 工場側デフォルトはAuto (オート) である。 スロット/ポートで"All"オプションに適用された選択がすべての該当インターフェイスのみに適用される。

Link Trap/リンク･トラップ - このオブジェクトはリンク･ステータスが変化したときトラップを送るかを定義する。 デフォルト設定は有効化されている。 .

Flow Control/フロー制御 - 選択されたインターフェイスでフロー制御を有効化または無効化するために使用される。

構成可能データ

Downlink Isolation/リンクダウンアイソレーション - プルダウン･メニューでポートのリンクダウンアイソレーションを有効化または無効化する。

Maximum Frame Size - イーサネット･ヘッダー、CRC、ペイロードを含みインターフェイスがサポートするまたは構成された最大イーサネット･フレーム･サイズ (1518から 9216). デフォルト最大フレーム･サイズは1518である。

Capability/機能 - 自動ネゴシエーション中に所与のインターフェイスのポート機能を通知できる。

Port Description/ポートの内容 - ポートに付属する内容説明文字列。 最大64文字まで可能である。

構成不可能なデータ

Port Type/ポート･タイプ - 普通のポートではこの欄は空白となる。 可能な値:

– Source/ソース - ポートは監視ポートである。 詳細はポート監視画面に出ている。

– Destination/ターゲット - ポートは監視ポートである。 詳細はポート監視画面に出ている。

– LAG - ポートはリンクアグリゲーション･トランクのメンバーである。 詳細はLAG画面に出ている。

E-KEY･ステータス - E-KEY･ステータスを示す。

Physical Status/物理ステータス - ポート速度と二重モードを示す。

Link Status/リンク･ステータス - リンクがアップかダウンかを示す。

ifIndex/インターフェイス番号 - このポートと関連付けられたインターフェイス･テーブルの番号。

コマンドボタン

Apply - IBP を入力値で更新する。 パワー･サイクル後、新たな値を保持させるには、保存を実行しなければならない。

8.3.7.2 サマリ

Port

Config | Summary | Mirroring

Unit/Slot/Port	Port Type	Forwarding State	Admin Mode	E-Keying Status	Physical Mode
Encl-CB1/0/1		Disabled	Disable	Connected	Auto
Encl-CB1/0/2		Disabled	Disable	Connected	Auto
Encl-CB1/0/3		Disabled	Disable	Connected	Auto
Encl-CB1/0/4		Disabled	Disable	Connected	Auto
Encl-CB1/0/5		Disabled	Disable	Connected	Auto
Encl-CB1/0/6		Disabled	Disable	Connected	Auto
Encl-CB1/0/7		Disabled	Disable	Connected	Auto
Encl-CB1/0/8		Disabled	Disable	Connected	Auto
Encl-CB1/0/9		Disabled	Disable	Connected	Auto
Encl-CB1/0/10		Disabled	Disable	Connected	Auto
Encl-CB1/0/11		Disabled	Disable	Connected	Auto
Encl-CB1/0/12		Disabled	Disable	Connected	Auto
Encl-CB1/0/13		Disabled	Disable	Connected	Auto
Encl-CB1/0/14		Disabled	Disable	Connected	Auto
Encl-CB1/0/15		Disabled	Disable	Connected	Auto
Encl-CB1/0/16		Disabled	Disable	Connected	Auto
Encl-CB1/0/17		Disabled	Disable	Connected	Auto
Encl-CB1/0/18		Disabled	Disable	Connected	Auto
Encl-CB1/0/19		Disabled	Disable	Connected	Auto
Encl-CB1/0/20		Disabled	Disable	Connected	Auto
Encl-CB1/0/21		Disabled	Disable	Connected	Auto
Encl-CB1/0/22		Disabled	Disable	Connected	Auto
Encl-CB1/0/23		Disabled	Disable	Connected	Auto
Encl-CB1/0/24		Disabled	Disable	Connected	Auto

図 : ポート･サマリ

この画面はボックス内のすべてのポートの状態を表示する。

構成不可のポート･ステータス･データ

Slot/Port / スロット/ポート - ポートを識別する。

Port Type/ポート･タイプ - 普通のポートではこの欄は空白となる。 可能な値:

– Source/ソース - ポートは監視ポートである。 詳細はポート監視画面に出ている。

– **Destination/ターゲット** - ポートは監視ポートである。 詳細はポート監視画面に出ている。

– **LAG** - ポートはリンクアグリゲーション・トランクのメンバーである。 詳細はLAG画面に出ている。

Forwarding State/転送ステート - ポートの現在のステートがスパニング・ツリー・ステートである。 このステートはフレーム受信時にポートが行う動作を制御する。 ブリッジがポート障害を検出すると、そのポートを故障状態に置く。 他の5個のステートは次のIEEE 802.1Dに定義される項目である：

– 無効

– ブロッキング

– リスニング

– ラーニング

– 転送

Admin Mode/管理モード - ポート制御管理ステート。 ポートはネットワークに許可されるには有効化されていなければならない。 デフォルト設定は有効化されている。

E-KEY・ステータス - ポートのE-KEY・ステータスを示す。

Physical Status/物理ステータス - ポート速度と二重モードを示す。 自動ネゴシエーション・モードでは二重モードと速度は自動ネゴシエーションで設定される。

Physical Status/物理ステータス - ポート速度と二重モードを示す。

Link Status/リンク・ステータス - リンクがアップかダウンかを示す。

Link Trap/リンク・トラップ - リンク状態の変化時にポートがトラップを送るかを示す。

ifIndex/インターフェイス番号 - このポートと関連付けられたインターフェイス・テーブルの番号。

Flow Control/フロー制御 - このポートでのフロー制御の状態を示す。

Downlink Isolation/リンクダウンアイソレーション - ポートのリンクダウンアイソレーション状態を示す。

Capability/機能 - 自動ネゴシエーション中のポート機能を示す。

Port Description/ポート内容 - ポートの内容を示す。

コマンドボタン

Refresh/更新 - 画面を最新データで更新する。

8.3.7.3 ミラーリング

図 ： ポート・ミラーリング

選択基準

Session ID/セッションID - リストからポート・ミラーリング・セッションを選択する。 許可されるセッション数はプラットフォームに依存する。 デフォルトでは最初のセッションが選択されている。 最大1個のセッションがサポートされる。

Mode/モード - 選択されたセッションIDのセッション・モードを指定する。デフォルトのセッション・モードは無効化である。

Destination Port/ターゲット・ポート - プローブ・ポートとして機能し、構成されたミラー化ポートからすべてのトラフィックを取得する。 デフォルト値は空白である。

構成可能データ

Source Port(s)/ソース・ポート - 方向性ソース・ポートをミラー・ポートとして指定する。 ソース・ポートのトラフィックがプローブ・ポートに送られる。 最大368ソース・ポートをセッション毎に選択できる。

コマンドボタン

Add Source Ports/ソース・ポートを追加する - 選択されたセッションにソース・ポートを追加する。

Remove Source Ports/ソース・ポートを削除する - 選択されたセッションの構成されたソース・ポートを削除する。

Apply - 更新された画面をIBPに送りIBPで変更を有効化する。

Delete/削除 - 選択されたセッション構成を削除する。

© 2010 富士通テクノロジー・ソリューションズ

8.3.8 ポート·チャネル

8.3.8.1 構成

Port Channel

Config | Status

Port Channel Name: Create Apply Refre

Unit/Slot/Port	Port Channel Name	Link Trap	Administrative Mode	Static Capability Mode	Link Status	Load Balance
		Enable	Enable	Disable		Source MAC address

Page		1
Unit/Slot/Port	Participation	Membership Conflicts
Encl-CB1/0/1	Exclude	
Encl-CB1/0/2	Exclude	
Encl-CB1/0/3	Exclude	
Encl-CB1/0/4	Exclude	
Encl-CB1/0/5	Exclude	
Encl-CB1/0/6	Exclude	
Encl-CB1/0/7	Exclude	
Encl-CB1/0/8	Exclude	
Encl-CB1/0/9	Exclude	
Encl-CB1/0/10	Exclude	
Encl-CB1/0/11	Exclude	
Encl-CB1/0/12	Exclude	
Encl-CB1/0/13	Exclude	
Encl-CB1/0/14	Exclude	
Encl-CB1/0/15	Exclude	
Encl-CB1/0/16	Exclude	
Encl-CB1/0/17	Exclude	
Encl-CB1/0/18	Exclude	
Encl-CB1/0/19	Exclude	

図： ポート·チャネル·コンフィグ

選択基準

Port Channel Name/ポート·チャネル名 - この画面で既存のポートチャネルを再構成するまたは新たなポートチャネルを生成できる。 このプルダウン·メニューから既存ポート·チャネルを選択する、または'Create'を選択して新ポート·チャネルを追加できる。 最大64個のポート·チャネルまで可能である。

Link Trap/リンク·トラップ - リンク·ステータスの変化時にトラップを送らせるかを指定する。 工場側デフォルトは有効化されており、トラップは送られる。

Admin Mode/管理モード - プルダウン·メニューから有効化または無効化を選択する。 ポート·チャネルが無効化されているときは、トラフィックは起こらず、LACPDUは落とされるが、ポート·チャネルを構成するリンクは解放されない。 デフォルト設定は有効化されている。

Static Capability Mode/静的機能モード - プルダウン·エントリ欄で対応行を選択して有効化または無効化できる。 工場側デフォルトは無効化されている。 この欄は読みのみのユーザーには構成できない。

Load Balance/負荷分散 - インターフェイス·ポート·チャネルに負荷分散モードを構成する。 とりうる値：

- Source MAC address/ソースMACアドレス - モードをソースMACアドレスに設定する。
- Destination MAC address/ターゲットMACアドレス - モードをターゲットMACアドレスに設定する。
- Source and destination MAC address/ソースとターゲットMACアドレス - モードをソースとターゲットMACアドレスに設定する。
- Source IP address/ソースIPアドレス - モードをソースIPアドレスに設定する。
- Destination IP address/ターゲットIPアドレス - モードをターゲットIPアドレスに設定する。

© 2010 富士通テクノロジー·ソリューションズ

– Source and destination IP address/ソースとターゲットIPアドレス - モードをソースとターゲットIPアドレスに設定する。

Participation/参加 -ポート毎にポート･チャネルのメンバーにするかを指定する。 デフォルトはexclude/除外である。 ポート･チャネルには最大8ポートまで割当てることができる。

構成可能データ

Port Channel Name/ポート･チャネル名 - ポート･チャネルに割当てる名前を入力する。 最大15文字の英数字からなるお好きな文字列を入力できる。 有効な名前はポート･チャネル生成のために必ず指定すること。

構成不可能なデータ

Slot/Port / スロット/ポート - 構成されるポート･チャネルのスロット/ポート識別。 この欄は新ポート･チャネル生成の際は表示されない。

Link Status/リンク･ステータス - リンクがアップかダウンかを示す。

Port Channel Members/ポート･チャネル･メンバー - スロット/ポート形式によるポート･チャネル･メンバーのリスト。

Membership Conflicts/メンバーシップの競合 - すでに他のポート･チャネル･メンバーであるポートを示す。 1個のポートは同時に1個のみのポート･チャネル･メンバーになれる。 このエントリが空白であれば、そのポートはどのポート･チャネルのメンバーでもない。

コマンドボタン

Apply - IBPを画面の値で更新する。IBPにパワー･サイクル後、設定を保持させるには、保存を実行しなければならない。. .。.

Delete/削除 - 現在選択されている構成されたポート･チャネルを削除する。 このポート･チャネルのメンバーであったすべてのポートはポート･チャネルから削除され、デフォルトVLANに含まれる。 この欄は新ポート･チャネル生成の際は表示されない。

Refresh/更新 - IBPにある現在のデータ･ステートにより画面のデータを更新する。

8.3.8.2 ステータス

Port Channel

Config | Status

Port Channel	Port Channel Name	Port Channel Type	Admin Mode	Static Capability Mode	Link State	Link Trap	Configured Ports	Active Ports	Load Balance

図 ： ポート･チャネル･ステータス

構成不可能なデータ

Port Channel/ポート･チャネル - ポート･チャネルのスロット/ポート識別。

Port Channel Name/ポート･チャネル名 - ポート･チャネルの名前。

Port Channel Type/ポート･チャネル･タイプ - このポート･チャネルのタイプ。

Admin Mode/管理モード - ポート･チャネルの管理モード、有効化または無効化である。

Static Capability Mode/静的機能モード - ポート･チャネルの静的機能モード、有効化または無効化である。

Link Status/リンク･ステータス - リンクがアップかダウンかを示す。

Link Trap/リンク･トラップ - リンク･ステータスの変化時にトラップを送るかを指定する。 デフォルト設定は有効化されている。

Configured Ports/構成されたポート - スロット/ポート形式によるポート·チャネルのメンバーであるポートのリスト。 ポート·チャネルには最大8ポートまで割当てることができる。

Active Ports/アクティブなポート - スロット/ポート形式によるポート·チャネルのアクティブに参加するメンバーであるポートのリスト。 ポート·チャネルには最大8ポートまで割当てることができる。

負荷分散 - 負荷分散モード情報を表示する。 とりうる値:

- Source MAC address/ソースMACアドレス - モードをソースMACアドレスに設定する。
- Destination MAC address/ターゲットMACアドレス - モードをターゲットMACアドレスに設定する。
- Source and destination MAC address/ソースとターゲットMACアドレス - モードをソースとターゲットMACアドレスに設定する。
- Source IP address/ソースIPアドレス - モードをソースIPアドレスに設定する。
- Destination IP address/ターゲットIPアドレス - モードをターゲットIPアドレスに設定する。.
- Source and destination IP address/ソースとターゲットIPアドレス - モードをソースとターゲットIPアドレスに設定する。

8.3.9　ポート･バックアップ

ポート･グループが生成されると2個のリンク･アグリゲーション･グループがそのポート･グループに関連付けられる。 2個のリンク･アグリゲーション･グループは内部でアクティブなバックアップ･ポートとして定義される。 2個のリンク･アグリゲーション･グループのうち1個は同時にアクティブ化される。 たとえば、アクティブなリンク･アグリゲーション･グループがリンク･アップであると、バックアップ･アグリゲーション･グループは遮断される(トラフィックの送受信は起こらない) 。 その他の場合、アクティブなアグリゲーション･グループがリンクダウンであれば (アクティブなアグリゲーション･グループの全メンバーがリンクダウン)、バックアップ･アグリゲーション･グループはアクティブ化される。 アクティブ集約グループがリンクアップに戻ると、バックアップ集約グループはアクティブでなくなる。

8.3.9.1　構成

Port Backup

Config | Status

Page		1	
Unit/Slot/Port	Uplink Set Name	Status	Active/Backup
Encl-CB1/0/37			
Encl-CB1/0/38			
Encl-CB1/0/39	default	Active	Active
Encl-CB1/0/40	default	Active	Active
Encl-CB1/0/41	default	Active	Active
Encl-CB1/0/42	default	Active	Active
Encl-CB1/0/43	default	Active	Active
Encl-CB1/0/44	default	Active	Active
Encl-CB1/0/45	default	Active	Active
Encl-CB1/0/46	default	Active	Active

Apply

図 ：　ポート･バックアップ･コンフィグ

構成可能データ

Active/Backup ｜ アクティブ/バックアップ - インターフェイスをアクティブなアグリゲーション･グループまたはバックアップ･アグリゲーション･グループに設定する欄を選択する。

構成不可能なデータ

Slot/Port｜ スロット/ポートポートを識別する。

Uplink Set Name/アップリンク･セット名 -　このインターフェイスが属するアップリンク･セットの名前。

Status / ｽﾃｰﾀｽ -アクティブまたはバックアップ。

コマンドボタン

Apply – IBPを画面の値で更新する。IBPにパワー･サイクル後、設定を保持させるには、保存を実行しなければならない。. .。

8.3.9.2　ｽﾃｰﾀｽ

この頁は現在構成されたすべてのポート･バックアップの状態を表示する。

Port Backup

Config | Status

Uplink Set Name	External Active Ports			External Backup Ports	Port Backup	Failback Time	Current Activated Port
default	Encl-CB1/0/39	Encl-CB1/0/40	Encl-CB1/0/41		Disable	60	
	Encl-CB1/0/42	Encl-CB1/0/43	Encl-CB1/0/44				
	Encl-CB1/0/45	Encl-CB1/0/46					

Refresh

図 : ポート･バックアップ･ステータス

構成不可能なデータ

Uplink Set Name/アップリンク･セット名 - アップリンク･セット名。

External Active Ports/アクティブな外部ポート - 構成されたアクティブな外部ポート。

External Backup Ports/外部バックアップポート - 構成された外部バックアップ･ポート。

Port Backup/ポート･バックアップ - アップリンク･セットの現在のポート･バックアップ設定。(有効化または無効化)

Failback Time/フェイルバック時間 - アクティブなポートのリンクが再開された場合アクティブなポートをアクティブ化するまでの遅延時間。

Current Activated Port/現在アクティブ化されているポート - アップリンク･セットの現在アクティブなポート。

8.4 セキュリティ・メニュー

この節は、802.1x、 Radius、TACACS＋、LDAP、 アクセス制御リスト、IPフィルター、https、セキュアシェル等IBPセキュリティの構成方法を説明する。

8.4.1 ポート・アクセス制御

8.4.1.1 構成



図 ： ポート・アクセス制御コンフィグ

選択基準

Administrative Mode/管理モード - このセレクタは管理モードの2つのオプションをリストする: 有効化と無効化である。 デフォルト値は無効化である。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。 .

8.4.1.2 ポート・コンフィグ

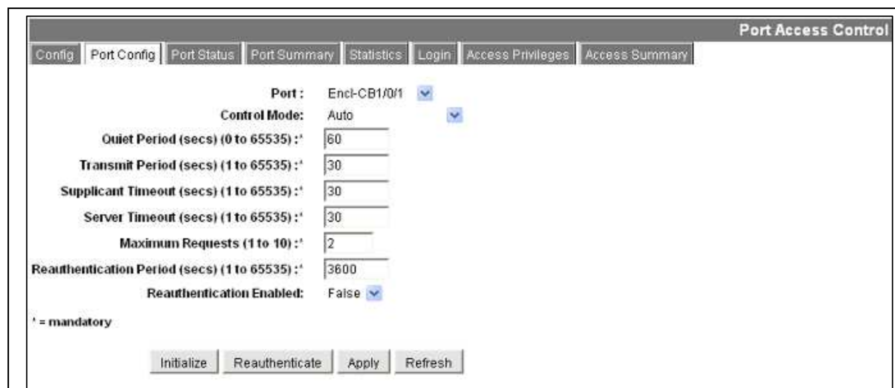


図 ： ポート・アクセス制御ポート・コンフィグ

選択基準

Port/ポート - 構成すべきポートを選択する。 この選択が変更されると、画面が更新されてすべての欄は新たに選択されたポートに更新される。 すべての物理インターフェイスは有効である。

Control Mode / 制御モード - このセレクタは制御モードのオプションをリストする。 制御モードはポートのリンク・ステータスがリンクアップである場合のみ設定される。 オプション：

– 非認証強制: 認証コード･ポート･アクセス･エンティティ (PAE)は制御されるポートを無条件に非認証に設定する。

– 認証強制: 認証コード･ポート･アクセス･エンティティ (PAE)は制御されるポートを無条件に認証に設定する。

– Auto (オート) : 認証コードPAEはポート･モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Reauthentication Enabled/再認証有効化 - この選択欄から指定されたポートの認証請求者を再認証するかを有効化または無効化できる。 選択可能な値は'true'/真と'false'/偽である。 再認証はこの値が'true'/真のときに行われる。 真でなければ再認証は許可されない。 デフォルト値は'false'/偽である。 この選択を変えてもApplyボタンを押すまでは構成は変化しない。

構成可能データ

Quiet Period/静止時間 - この選択欄から選択されたポートに静止時間を構成できる。 このコマンドはこのポートで認証コードステート･マシンが使用するタイマーの秒単位の値を認証請求者を取得しようとしない時間に設定する。 静止時間とは、認証請求者との認証交換の失敗後、認証コード認証請求者を取得しようとしない時間である。 静止時間は0と65535の間の数字とする。静止時間が0とは認証コードステート･マシンは認証請求者を取得することはないことを意味する。 デフォルト値は60である。この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Transmit Period/送信時間 - この入力欄から選択されたポートに送信時間を構成できる。 送信時間は、認証請求者にEAPOL EAP要求/アイデンティティ･フレームをいつ送るかを決めるための、指定されたポートで認証コードステート･マシンが使用するタイマーの秒単位の値である。 送信時間は1から65535の範囲の数字とする。デフォルト値は 30である。この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Supplicant Timeout/認証請求者タイムアウト - この入力欄から選択されたポートに認証請求者タイムアウトを入力できる。 この認証請求者タイムアウトは認証請求者をタイムアウトするまでの、指定されたポートで認証コードステート･マシンが使用するタイマーの秒単位の値である。 認証請求者タイムアウトは1から65535の範囲の数字とする。デフォルト値は30である。 この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Server Timeout/サーバ･タイムアウト - この入力欄から選択されたポートにサーバ･タイムアウトを入力できる。 サーバ･タイムアウトは認証サーバをタイムアウトするまでの、指定されたポートで認証コードが使用するタイマーの秒単位の値である。 サーバ･タイムアウトは1から65535の範囲の数字とする。デフォルト値は30である。 この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Maximum Requests/最大要求回数 - この入力欄から選択されたポートに最大要求回数を入力できる。最大要求回数値は認証請求者をタイムアウトするまでのEAPOL EAP要求/アイデンティティをこのポートで認証コードステート･マシンが再送する最大回数である。 最大要求回数は1から10の範囲の数字とする。デフォルト値は2である。 この値を変化させてもApplyボタンを押すまでは構成を変更しない。

Reauthentication Period/再認証時間 - この入力欄から選択されたポートに再認証時間を入力できる。再認証時間は認証請求者の再認証が行われる時を定める、指定されたポートで認証コードステート･マシンが使用するタイマーの秒単位の値である。 再認証時間は1から65535の範囲の数字とする。デフォルト値は3600である。この値を変化させてもApplyボタンを押すまでは構成を変更しない。

コマンドボタン

Initialize/初期化 - このボタンは選択されたポートで初期化シーケンスを開始する。 このボタンは制御モードが'Auto (オート) 'である場合のみ選択できる。 このボタンが選択不可の場合はグレイアウトされ何もできない。 このボタンを押すと、動作は直ちに適用される。 この動作が生じるにはApplyボタンを押す必要がない。

Reauthenticate/再認証 - このボタンは選択されたポートで再認証シーケンスを開始する。 このボタンは制御モードが'Auto (オート) 'である場合のみ選択できる。 このボタンが選択不可の場合はグレイアウトされ何もできない。 このボタンを押すと、動作は直ちに適用される。 この動作が生じるにはApplyボタンを押す必要がない。

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。

Refresh/更新 - デフォルト値は3600である。

8.4.1.3 ポートステータス

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Port:	Encl-CB1/0/1
Control Mode:	Auto
Quiet Period (secs):	60
Transmit Period (secs):	30
Supplicant Timeout (secs):	30
Server Timeout (secs):	30
Maximum Requests :	2
Reauthentication Period (secs):	3600
Reauthentication Enabled:	False
Control Direction:	Both
Protocol Version:	1
PAE Capabilities:	Authenticator
Authenticator PAE State:	Initialize
Backend State:	Initialize

Refresh

図 : ポート・アクセス制御ポート・ステータス

選択基準

Port/ポート -表示すべきポートを選択する。 この選択が変更されると、画面が更新されてすべての欄は新たに選択されたポートに更新される。 すべての物理インターフェイスは有効である。

構成不可能なデータ

Control Mode / 制御モード指定されたポートに構成された制御モードを表示する。 オプション:

- 非認証強制:
- 認証コード・ポート・アクセス・エンティティ (PAE)は制御されるポートを無条件に非認証に設定する
- 認証強制: 認証コード・ポート・アクセス・エンティティ (PAE)は制御されるポートを無条件に認証に設定する。
- Auto (オート) :認証コードPAEはポート・モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Quiet Period/静止時間 -このフィールドは選択されたポートに構成された静止時間を表示する。 この静止時間は認証請求者を取得しようとしない時間を定めるこのポートで認証コードステート・マシンが使用するタイマーの秒単位の値である。 静止時間とは、認証請求者との認証交換の失敗後、認証コード認証請求者を取得しようとしない時間である。 静止時間は0から65535の範囲の数字である。

Transmit Period/送信時間 -このフィールドは選択されたポートに構成された送信時間を表示する。 送信時間は、認証請求者にEAPOL EAP要求/アイデンティティ・フレームをいつ送るかを決めるための、指定されたポートで認証コードステート・マシンが使用するタイマーの秒単位の値である。 送信時間は1から65535の範囲の数字である。

Supplicant Timeout/認証請求者タイムアウト -このフィールドは選択されたポートに構成された認証請求者タイムアウトを表示する。 この認証請求者タイムアウトは認証請求者をタイムアウトするまでの、指定されたポートで認証コードステート・マシンが使用するタイマーの秒単位の値である。 認証請求者タイムアウトは1から65535の範囲の数字である。

Server Timeout/サーバ･タイムアウト -このフィールドは選択されたポートに構成されたサーバ･ムアウトを表示する。 サーバ･タイムアウトは認証サーバをタイムアウトするまでの、指定されたポートで認証コードが使用するタイマーの秒単位の値である。 認証請求者タイムアウトは1から65535の範囲の数字である。

Maximum Requests/最大要求回数 - この欄は選択されたポートへの構成された最大要求回数を表示する。 最大要求回数値は認証請求者をタイムアウトするまでのEAPOL EAP要求/アイデンティティをこのポートで認証コードステート･マシンが再送する最大回数である。 最大要求回数は1から10までの値である。

Reauthentication Period/再認証時間 - この欄は選択されたポートに構成された再認証時間を表示する。 再認証時間は認証請求者の再認証が行われる時を定める、指定されたポートで認証コードステート･マシンが使用するタイマーの秒単位の値である。 認証請求者タイムアウトは1から65535の範囲の数字である。

Reauthentication Enabled/再認証有効化 - この欄は選択されたポートに再認証が有効化されているかを表示する。 この欄は構成できる。 可能な値は'true'/真と'false'/偽である。 再認証はこの値が'true'/真のときに行われる。 真でなければ再認証は許可されない。

Control Direction/制御方向 - 指定されたポートでの制御方向を表示する。 制御方向は認証請求者と認証コードの間で行われるプロトコル交信のレベルを決定する。 これは未認証の被制御ポートが両方向通信(入出フレームを両方とも無効化) またはインバウンドのみか(インバウンド･フレームの受信を無効化)を制御するかに影響する。 この欄は一部のプラットフォームでは構成できない。

Protocol Version/プロトコル･バージョン - この欄は選択されたポートに関連付けられたプロトコル･バージョンを表示する。 1のみ可能な値であり、これは802.1x規格の最初のバージョンに対応する。 この欄は構成できない。

PAE Capabilities/PAE機能 - この欄は選択されたポートのポート･アクセス･エンティティ(PAE)の機能を表示する。 とりえる値は"Authenticator"(認証コード)または"Supplicant"(認証請求者) である。 この欄は構成できない。

Authenticator PAE State/認証コードPAEのステート - この欄は認証コードPAEのステート･マシンの現状を表示する。 とりうる値：

- "Initialize" (初期化)
- "Disconnected" (非接続)
- "Connecting"(接続中)
- "Authenticating"(認証中)
- "Authenticated"(認証完了)
- "Aborting"(中止中)
- "Held"(一時停止中)
- "ForceAuthorized"(強制認証)
- "ForceUnauthorized"(強制非認証)

Backend Authentication State/バックエンド認証ステート - この欄はバックエンド認証ステート･マシンの現状を表示する。 とりうる値：

- "Request"(要求)
- "Response"(応答)
- "Success"(成功)
- "Fail"(失敗)
- "Timeout"(タイムアウト)
- "Initialize" (初期化)
- "Idle"(アイドル)

コマンドボタン

Refresh/更新 - デフォルト値は3600である。

8.4.1.4 ポート・サマリ

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Port Status
Encl-CB1/0/1	Auto	Auto	False	Authorized
Encl-CB1/0/2	Auto	Auto	False	Authorized
Encl-CB1/0/3	Auto	Auto	False	Authorized
Encl-CB1/0/4	Auto	Auto	False	Authorized
Encl-CB1/0/5	Auto	Auto	False	Authorized
Encl-CB1/0/6	Auto	Auto	False	Authorized
Encl-CB1/0/7	Auto	Auto	False	Authorized
Encl-CB1/0/8	Auto	Auto	False	Authorized
Encl-CB1/0/9	Auto	Auto	False	Authorized
Encl-CB1/0/10	Auto	Auto	False	Authorized
Encl-CB1/0/11	Auto	Auto	False	Authorized
Encl-CB1/0/12	Auto	Auto	False	Authorized
Encl-CB1/0/13	Auto	Auto	False	Authorized
Encl-CB1/0/14	Auto	Auto	False	Authorized
Encl-CB1/0/15	Auto	Auto	False	Authorized
Encl-CB1/0/16	Auto	Auto	False	Authorized
Encl-CB1/0/17	Auto	Auto	False	Authorized
Encl-CB1/0/18	Auto	Auto	False	Authorized
Encl-CB1/0/19	Auto	Auto	False	Authorized
Encl-CB1/0/20	Auto	Auto	False	Authorized
Encl-CB1/0/21	Auto	Auto	False	Authorized
Encl-CB1/0/22	Auto	Auto	False	Authorized
Encl-CB1/0/23	Auto	Auto	False	Authorized
Encl-CB1/0/24	Auto	Auto	False	Authorized
Encl-CB1/0/25	Auto	Auto	False	Authorized
Encl-CB1/0/26	Auto	Auto	False	Authorized

図 : ポート・アクセス制御ポート・サマリ

構成不可能なデータ

Port/ポート -現在のテーブル行に設定が表示されるポートを指定する。

Control Mode / 制御モード - この欄はポートの構成された制御モードを示す。 とりうる値:

- 非認証強制: 認証コード・ポート・アクセス・エンティティ (PAE)は制御されるポートを無条件に非認証に設定する
- 認証強制: 認証コード・ポート・アクセス・エンティティ (PAE)は制御されるポートを無条件に認証に設定する。
- Auto (オート) : 認証コードPAEはポート・モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Operating Control Mode/動作制御モード - この欄はポートが現在動作中の制御モードを示す。 とりうる値:

- "ForceUnauthorized"(強制非認証)
- "ForceAuthorized"(強制認証)
- Auto (オート)
- N/A: ポートが外された状態にあるとポート・アクセス制御には参加できない。

Reauthentication Enabled/再認証有効化 - この欄は指定されたポートの認証請求者の再認証が許可されているかを示す。 可能な値は'true'/真と'false'/偽である。 再認証はこの値が'true'/真のときに行われる。 真でなければ再認証は許可されない。 .

Port Status /ポートステータス- この欄は指定されたポートの認証状態を示す。 とりうる値は'Authorized'(認証された), 'Unauthorized'(拒否された)および'N/A'(不明)である。 ポートが外された状態にあると、ポートはポート･アクセス制御に参加できないのでこの値は'N/A'になる。

コマンドボタン

Refresh/更新 - ページ情報を更新する。

8.4.1.5 統計

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Port:	Encl-CB1/0/1
EAPOL Frames Received:	0
EAPOL Frames Transmitted:	0
EAPOL Start Frames Received:	0
EAPOL Logoff Frames Received:	0
Last EAPOL Frame Version:	0
Last EAPOL Frame Source:	00:00:00:00:00:00
EAP Response/ID Frames Received:	0
EAP Response Frames Received:	0
EAP Request/ID Frames Transmitted:	0
EAP Request Frames Transmitted:	0
Invalid EAPOL Frames Received:	0
EAPOL Length Error Frames Received:	0

Refresh | Clear All | Clear

図 : ポート･アクセス制御統計

選択基準

Port/ポート - 表示すべきポートを選択する。この選択が変更されると、画面が更新されてすべての欄は新たに選択されたポートに更新される。 すべての物理インターフェイスは有効である。

構成不可能なデータ

EAPOL Frames Received/受信されたEAPOLフレーム - 認証コードが受信した有効な任意のタイプのEAPOLフレーム数を表示する。

EAPOL Frames Transmitted/送信されたEAPOLフレーム - 認証コードが送信した有効な任意のタイプのEAPOLフレーム数を表示する。

EAPOL Start Frames Received/受信されたEAPOL開始フレーム - 認証コードが受信した有効な任意のタイプのEAPOL開始フレーム数を表示する。

EAPOL Logoff Frames Received/受信されたEAPOLログオフ･フレーム - 認証コードが受信した有効な任意のタイプのEAPOLログオフ･フレーム数を表示する。

Last EAPOL Frame Version/直前のEAPOLフレーム･バージョン - 直前に受信されたEAPOLフレームに運ばれたプロトコル･バージョン番号を表示する。

Last EAPOL Frame Source/直前のEAPOLフレーム･ソース - 直前に受信されたEAPOLフレームに運ばれたソースMACアドレスを表示する。

EAPOL Response/Id Frames Received/受信されたEAPOL応答/IDフレーム - 認証コードが受信したEAP応答/IDフレーム数を表示する。

EAP Response Frames Received/受信されたEAP応答フレーム - 認証コードが受信した有効なEAP応答フレーム数(応答/IDフレーム以外)を表示する。

EAP Request/Id Frames Transmitted/送信されたEAP応答/IDフレーム - 認証コードが送信したEAP応答/IDフレーム数を表示する。

EAP Request Frames Transmitted/送信されたEAP要求フレーム - 認証コードが送信したEAP要求フレーム数(応答/IDフレーム以外)を表示する。

Invalid EAPOL Frames Received/受信された無効なEAPOLフレーム - フレーム･タイプが認識されずに認証コードが受信したEAPOLフレーム数を表示する。

EAP Length Error Frames Received/受信されたEAP長エラー･フレーム - フレーム･タイプが認識されずに認証コードが受信したEAPOLフレーム数を表示する。

コマンドボタン

Refresh/更新 - デフォルト値は3600である。

Clear All/全クリア -このボタンはすべてのポートのすべての統計を0にリセットする。確認プロンプトは表示されない。 このボタンが押されると、統計は直ちに消去される。

Clear/クリア -このボタンは選択されたポートの統計をリセットする。 確認プロンプトは表示されない。 このボタンが押されると、統計は直ちに消去される。

8.4.1.6 ログイン

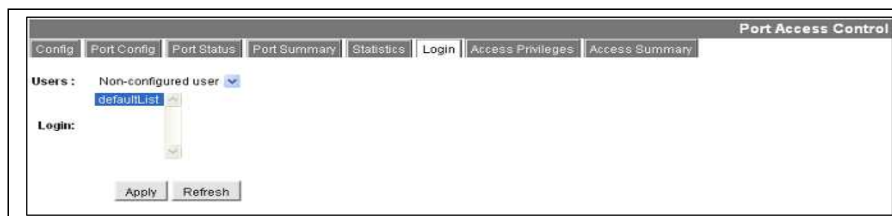


図 : ポート･アクセス制御ログイン

選択基準

Users/ユーザー - 802.1xポート･セキュリティに詮索されたログイン･リストを使用するユーザー名を選択する。

構成可能データ

Login / ログイン- 指定されたユーザーに適用されるログインを選択する。 すべての構成されたログインが表示される。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー･サイクル後、保持されない。

Refresh/更新 - デフォルト値は3600である。

8.4.1.7 アクセス特権

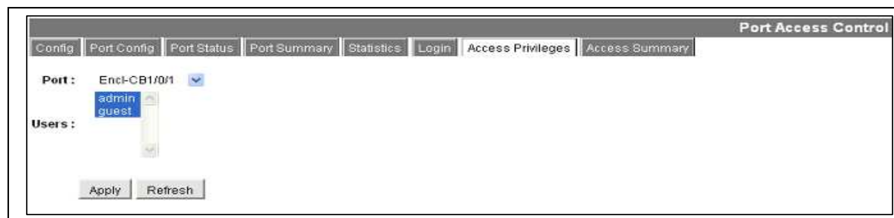


図 ： ポート･アクセス制御アクセス特権

選択基準

Port/ポート -構成するポートを選択する。

構成可能データ

Users/ユーザー - 指定されたポートにアクセスできるユーザーを選択する。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー･サイクル後、保持されない。

Refresh/更新 - デフォルト値は3600である。

8.4.1.8　　アクセス･サマリ

Port Access Control

Config | Port Config | Port Status | Port Summary | Statistics | Login | Access Privileges | Access Summary

Port	Users
Encl-CB1/0/1	admin guest
Encl-CB1/0/2	admin guest
Encl-CB1/0/3	admin guest
Encl-CB1/0/4	admin guest
Encl-CB1/0/5	admin guest
Encl-CB1/0/6	admin guest
Encl-CB1/0/7	admin guest
Encl-CB1/0/8	admin guest
Encl-CB1/0/9	admin guest
Encl-CB1/0/10	admin guest
Encl-CB1/0/11	admin guest
Encl-CB1/0/12	admin guest
Encl-CB1/0/13	admin guest
Encl-CB1/0/14	admin guest
Encl-CB1/0/15	admin guest
Encl-CB1/0/16	admin guest

図 ： ポート･アクセス制御アクセス･サマリ

構成不可能なデータ

Port/ポート -ポートをスロット/ポート形式で表示する。

Users/ユーザー - ポートにアクセスできるユーザーを表示する。

コマンドボタン

Refresh/更新 - デフォルト値は3600である。

8.4.2 ポート・セキュリティ

8.4.2.1 構成



図 ： ポート・セキュリティ・コンフィグ

構成可能データ

Port Security Mode/ポート・セキュリティ・モード - ポート・セキュリティ機能を有効化または無効化する。

コマンドボタン

Apply - 新構成を適用し変更は直ちに効力を発する。 当該変更は保存を実行しないと、パワー・サイクル後、保持されない。

8.4.2.2 インターフェイス・コンフィグ

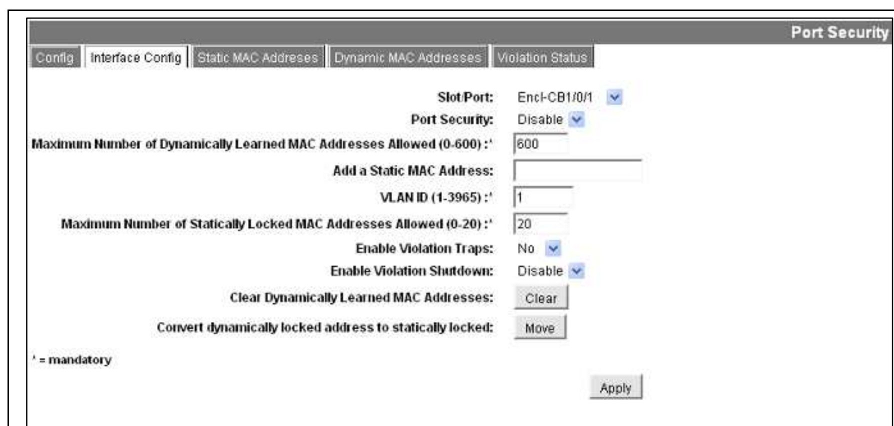


図 ： ポート・セキュリティ・インターフェイス・コンフィグ

選択基準

Slot/Port / スロット/ポート - 構成すべきポートを選択する。

Port Security Mode/ポート・セキュリティ・モード - 選択されたインターフェイスにポート・セキュリティ機能を有効化または無効化する。

Enable violation traps/バイオレーショントラップを有効化する - 許可されていないMACアドレスがあるパケットがロックされたポートで受信された際、新たなバイオレーショントラップ指定の送信を有効化または無効化する。

Enable Violation Shutdown/バイオレーションシャットダウンを有効化する - 選択されたインターフェイスにポート・セキュリティバイオレーションシャットダウン・モードを有効化または無効化する。

構成可能データ

Maximum Number of Dynamically Learned MAC Addresses Allowed/許可される動的学習MACアドレスの最大数 - 選択されたインターフェイスで動的学習MACアドレスの最大数を設定する。

Add a static MAC address/静的MACアドレスを追加する - 選択されたインターフェイスについてMACアドレスを静的にロックされたMACアドレス･リストに追加する。

VLAN ID - 選択されたインターフェイスについて静的にロックされたMACアドレス･リストに追加されるMACアドレスに対応するVLAN IDを追加する。

Maximum Number of Statically Learned MAC Addresses Allowed/許可される静的学習MACアドレスの最大数 - 選択されたインターフェイスで静的にロックされたMACアドレスの最大数を設定する。

コマンドボタン

Clear/クリア - 選択されたインターフェイスの動的MACアドレスを消去する。

Move/移動 - 動的学習MACアドレスを静的にロックされたアドレスに変換する。 動的MACアドレス･エントリは静的限界に到達するまで番号の昇順で静的MACアドレス･エントリに変換される。

Apply -新構成を適用し変更は直ちに効力を発する。 当該変更は保存を実行しないと、パワー･サイクル後、保持されない。

8.4.2.3 静的MACアドレス



図 ： ポート･セキュリティ静的MACアドレス

選択基準

Slot/Port / スロット/ポート - データを表示させる物理インターフェイスを選択する。

構成可能データ

MAC Address/MACアドレス - 削除するMACアドレスのユーザー入力を受け入れる。

VLAN ID - 削除するMACアドレスに対応するVLAN IDのユーザー入力を受け入れる。

構成不可能なデータ

MAC Address / MACアドレス- ユーザー定義の静的にロックされたMACアドレスを表示する。

VLAN ID - MACアドレスに対応するVLAN IDを表示する。

コマンドボタン

Apply - 新構成を適用し変更は直ちに効力を発する。 当該変更は保存を実行しないと、パワー･サイクル後、保持されない。

8.4.2.4 動的MACアドレス

図 ： ポート·セキュリティ動的MACアドレス

選択基準

Slot/Port / スロット/ポート - データを表示させる物理インターフェイスを選択する。

構成不可能なデータ

MAC Address/MACアドレス -特定のポートで学習されたMACアドレスを表示する。

VLAN ID - MACアドレスに対応するVLAN IDを表示する。

Number of Dynamic MAC addresses learned/学習された動的MACアドレス数 - 特定のポートで動的に学習されたMACアドレスの数を表示する。

8.4.2.5 バイオレションーンステータス

図 ： ポート·セキュリティ動的バイオレーションステータス

選択基準

Slot/Port / スロット/ポート - データを表示させる物理インターフェイスを選択する。

構成不可能なデータ

Last Violation MAC Address/直前のバイオレーションMAC - ロックされたポートで破棄された直前のパケットのソースMACアドレスを表示する。

VLAN ID - 直前のバイオレーションMACアドレスに対応するVLAN IDを表示する。

8.4.3 RADIUSを構成する

8.4.3.1 構成

Configuration

Config | Server Config | Accounting Server Config

Current Server:
Number of Configured Servers: 0
Max Number of Retransmits (1 to 15):* 4
Timeout Duration (secs) (1 to 30):* 5
Dead Time (secs) (1 to 255):* 255
Accounting Mode: Disable
Radius Attribute 4 (NAS-IP Address): 0 . 0 . 0 . 0

* = mandatory

Apply Refresh

図 ：RADIUS コンフィグ

選択基準

Accounting Mode/アカウンティング・モード - RADIUSアカウンティング・モードの有効化または無効化を選択する。

構成可能データ

Max Number of Retransmits/最大再送信数 - 要求パケットが再送信される最大の回数の値。 この値の範囲は1から15までである。RADIUS最大送信数とRADIUSタイムアウトを構成する際は最大遅延時間を検討すること。 複数のRADIUSサーバを構成する場合、各サーバの最大再送信数は次のサーバが試行される前に消化される。 再送信は、RADIUSサーバから応答が無く当該サーバに構成されたタイムアウト値が経過するまでは、行われない。 従って、RADIUSアプリケーションからの応答を受信する最大遅延時間はすべての構成されたサーバの(再送信時間タイムアウト)合計に等しい。 RADIUS要求がユーザーのログイン試行により生成された場合、すべてのユーザー・インターフェイスはRADIUSアプリケーションが応答を返すまでブロックされる。

Timeout Duration (secs)/タイムアウト時間 (秒) - 要求再送信の秒単位によるタイムアウト値。この値の範囲は1から30までである。RADIUS最大送信数とRADIUSタイムアウトを構成する際は最大遅延時間を検討すること。 複数のRADIUSサーバを構成する場合、各サーバの最大再送信数は次のサーバが試行される前に消化される。 再送信は、RADIUSサーバから応答が無く当該サーバに構成されたタイムアウト値が経過するまでは、行われない。 従って、RADIUSアプリケーションからの応答を受信する最大遅延時間はすべての構成されたサーバの(再送信時間タイムアウト)合計に等しい。 RADIUS要求がユーザーのログイン試行により生成された場合、すべてのユーザー・インターフェイスはRADIUSアプリケーションが応答を返すまでブロックされる。

静止時間 静止時間 – 秒単位の静止時間。 有効な範囲は1から255までである。

Radius Attribute 4 (NAS-IP Address)/Radius属性4 (NAS-IPアドレス) - Radius要求にRadius属性4 (NAS-IPアドレス)を含めることの有効化か無効化を選択する。 NAS-IPアドレスとしてRADIUSサーバに送られるIPアドレスを明示的に指定する。 指定されない場合、RADIUSサーバにパケットを送るために使用されるアウトバウンド・インターフェイスのIPアドレスがNAS-IPアドレスとして追加される。

構成不可能なデータ

Current Server/現在のサーバ - 現在のサーバのIPアドレスまたはホスト名。 この欄は構成されたサーバが無い場合は空白である。

Number of Configured Servers/構成されたサーバ数 - 構成されたRADIUSサーバの数。 このは0から3の範囲とすること。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。

Refresh/更新 - デフォルト値は3600である。

8.4.3.2 サーバ・コンフィグ

図 : RADIUS サーバ・コンフィグ

選択基準

RADIUS Server/RADIUS サーバ - 構成するRADIUS サーバを選択する。 サーバを追加するにはaddを選ぶ。

Primary Server/プライマリ・サーバ - 選択されたサーバをプライマリまたはセカンダリ・サーバに設定する。

Message Authenticator/メッセージ認証コード - 選択されたサーバのメッセージ認証コード属性を有効化または無効化する。

構成可能データ

IP Address/IPアドレス - 追加されたサーバのIPアドレス。
次のIPアドレスを使うことはできない:

- 0.0.0.0
- 255.255.255.255
- 224.xxx.xxx.xxx
- 127.0.0.1

Host Name/ホスト名 - 追加されたサーバのホスト名

Port/ポート - このサーバが使用するUDPポート。 有効な範囲は0から65535までである。

Secret/シークレット - このサーバに共有されるシークレット。 この欄は入力のみである。

Apply - シークレットはこのボックスがチェックオンされている場合のみ適用される。 このボックスがチェックオンされていない場合、シークレット欄に何を入力しても効果は無く保持されない。 この欄はユーザーが読み書き特権を持つ場合のみ表示される。

Encrypted/暗号化 - シークレット文字列が暗号化される際はこのボックスがチェックオンされていること。この欄はユーザーが読み書き特権を持つ場合のみ表示される。

構成不可能なデータ

Current/カレント - このサーバが現在認証サーバとして使用中であることを示す。

Secret Configured /シークレット構成- このサーバの共有シークレットが構成されたことを示す。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。 .

Remove/削除 - 選択されたサーバを構成から削除する。 このボタンは読み書き特権ユーザーにのみ利用できる。変更は保存を実行しなければパワー・サイクル後、保持されない。.

Refresh/更新 - デフォルト値は3600である。

8.4.3.3 アカウンティング・サーバ・コンフィグ

図 : RADIUS アカウンティング・サーバ・コンフィグ

選択基準

Accounting Server/アカウンティング・サーバ - データが表示されるまたは構成されるアカウンティング・サーバを選択する。 add item/項目を追加するが選択されると、新たなアカウンティング・サーバを構成できる。

構成可能データ

IP Address/IPアドレス - 追加するアカウンティング・サーバのIPアドレス。Add項目が選択されているときのみこの欄は構成できる。
次のIPアドレスを使うことはできない:

- 0.0.0.0
- 255.255.255.255
- 224.xxx.xxx.xxx
- 127.0.0.1

Host Name/ホスト名 - 追加されたサーバのホスト名

Port / /ポート -アカウンティング・サーバが使用するUDPポートを指定する。 有効な範囲は0から65535までである。読みのみ特権ユーザーには値は表示されるが変更はできない。

Secret/シークレット - 指定されたアカウンティング・サーバと使用する共有シークレットを指定する。 この欄はユーザーが読み書き特権を持つ場合のみ表示される。

Apply - シークレットはこのボックスがチェックオンされている場合のみ適用される。 このボックスがチェックオンされていない場合、シークレット欄に何を入力しても効果は無く保持されない。この欄はユーザーが読み書き特権を持つ場合のみ表示される。

Encrypted/暗号化 - シークレット文字列が暗号化される際はこのボックスがチェックオンされていること。 この欄はユーザーが読み書き特権を持つ場合のみ表示される。

構成不可能なデータ

Secret Configured /シークレット構成 -このアカウンティング･サーバにシークレットが構成されたことを示す。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー･サイクル後、保持されない。 .

Remove/削除 - 選択されたアカウンティング･サーバを構成から削除する。 このボタンは読み書き特権ユーザーにのみ利用できる。 変更は保存を実行しなければパワー･サイクル後、保持されない。

Refresh/更新 - デフォルト値は3600である。

© 2010 富士通テクノロジー･ソリューションズ

8.4.4 RADIUS 統計

8.4.4.1 RADIUS 統計

Statistics
Radius Statistics | Server Statistics | Accounting Server Statistics | Clear Statistics
Invalid Server Addresses: 0
Refresh

図 : RADIUS 統計

構成不可能なデータ

Invalid Server Addresses/無効なサーバ･アドレス - 未知のアドレスから受信された RADIUSアクセス･応答パケットの数。

コマンドボタン

Refresh/更新- デフォルト値は3600である。

8.4.4.2 サーバ統計

Statistics
Radius Statistics | Server Statistics | Accounting Server Statistics | Clear Statistics
RADIUS Server:
Round Trip Time (secs):
Access Requests:
Access Retransmissions:
Access Accepts:
Access Rejects:
Access Challenges:
Malformed Access Responses:
Bad Authenticators:
Pending Requests:
Timeouts:
Unknown Types:
Packets Dropped:
Refresh

図 : RADIUS サーバ統計

選択基準

RADIUS サーバ - 統計を表示するRADIUSサーバのIPアドレスまたはホスト名を選択する。

構成不可能なデータ

Round Trip Time (secs)/ラウンド･トリップ時間 - このRADIUS認証サーバにより一致した直前のアクセス-応答/アクセス-試行とアクセス-要求の間の100分の1秒単位の時間間隔。

アクセス要求 - このサーバに送られたRADIUSアクセス-要求パケット数。 この数は再送信を除く。

Access Retransmissions/アクセス再送信 - このサーバに再度送られたRADIUSアクセス-要求パケット数。

Access Accepts/アクセス許可数 -このサーバから受信された有効と無効パケットを含む、RADIUSアクセス-許可パケット数。

Access Rejects/アクセス拒否数 -このサーバから受信された有効と無効パケットを含む、RADIUSアクセス-拒否パケット数。

Access Challenges/アクセス試行数 -このサーバから受信された有効と無効パケットを含む、RADIUSアクセス-試行パケット数。

Malformed Access Responses/間違いアクセス応答 -このサーバから受信された間違いRADIUSアクセス-応答パケット数。 不正パケットは無効な長さのものを含む。 間違いアクセス-応答には、間違い認証コードまたは間違い署名属性または不明タイプは含まれない。

Bad Authenticators/間違い認証コード -このサーバから受信された無効認証コードまたは署名属性を含むRADIUSアクセス-応答パケット数。

Pending Requests/要求中 -まだタイムアウトしていないか応答を受けていないこのサーバをターゲットとするRADIUSアクセス-応答数。

Timeouts/タイムアウト回数 -このサーバへの認証タイムアウトの回数。

Unknown Types/不明なイプ -認証ポートでこのサーバから受信されたタイプが不明なRADIUSパケット数。

Packets Dropped/破棄パケット -認証ポートでこのサーバから受信され他の理由により落とされたRADIUSパケット数。

コマンドボタン

Refresh/更新 - デフォルト値は3600である。

8.4.4.3 アカウンティング・サーバ統計

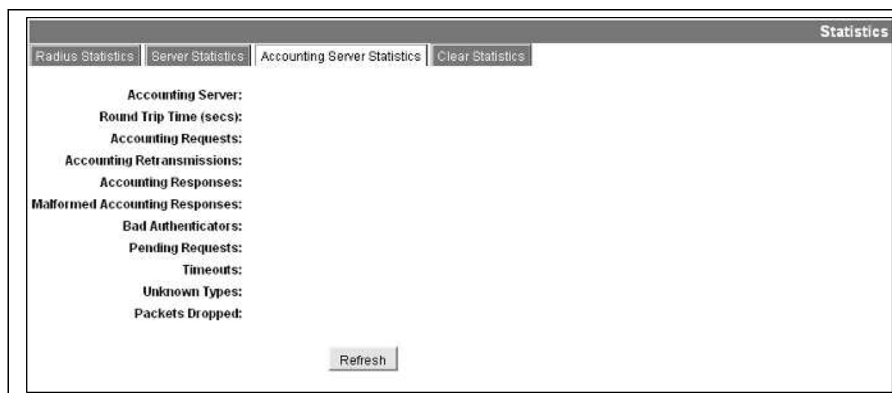


図 : RADIUS アカウンティング・サーバ統計

構成不可統計

Accounting Server/アカウンティング・サーバ - 統計と関連付けられたアカウンティング・サーバを識別する。

Round Trip Time (secs)/ラウンド・トリップ時間 - このRADIUSアカウンティング・サーバにより一致した直前のアクセス-応答とアクセス-要求の間の100分の1秒単位の時間間隔。

Accounting Requests/アカウンティング要求 - 再送信を除き送信されたRADIUSアカウンティング要求パケット数を表示する。

Accounting Retransmissions/アカウンティング再送信 -このRADIUSアカウンティング・サーバに再度送られたRADIUSアカウンティング-要求パケット数を表示する。

Accounting Responses/アカウンティング応答 - このサーバからアカウンティング・ポートで受信されたRADIUSパケット数を表示する。

© 2010 富士通テクノロジー・ソリューションズ

Malformed Accounting Responses/不正アカウンティング応答 -このサーバから受信された不正RADIUSアカウンティング-応答パケット数を表示する。 不正パケットは無効な長さのものを含む。 不正認証コードと不明タイプは不正アカウンティング応答に含まれない。

Bad Authenticators/不正認証コード - このアカウンティング･サーバから受信された無効な認証コードを含んだRADIUSアカウンティング-応答パケット数を示す。

Pending Requests/要求中 -まだタイムアウトしていないか応答を受けていないこのサーバをターゲットとするRADIUSアカウンティング-要求数。

Timeouts/タイムアウト回数 -このサーバへのアカウンティング･タイムアウトの回数を表示する。

Unknown Types/不明なイプ - アカウンティング･ポートでこのサーバから受信されたタイプが不明なRADIUSパケット数を表示する。

Packets Dropped/破棄パケット - アカウンティング･ポートでこのサーバから受信され他の理由により落とされたRADIUSパケット数を表示する。

コマンドボタン

Refresh/更新 - デフォルト値は3600である。

8.4.4.4 統計をクリアする



図 : RADIUS 統計のクリア

コマンドボタン

Clear All RADIUS Statistics/すべてのRADIUS 統計をクリアするr - このボタンはアカウンティング･サーバ、認証サーバ、RADIUS 統計を消去する。

8.4.5 TACACS+

8.4.5.1 コンフィグ

TACACS+
Config | Server Config
Key String (0 to 128 characters): •••••• ☐ Encrypted
Connection Timeout (1 to 30 secs):* 5
* = mandatory
Apply

図 : TACACS+ コンフィグ

構成可能データ

Key String/キー文字列 - デバイスとTACACS+サーバ間のTACACS+通信のための認証キーと暗号化キーを指定する。 有効な範囲は0から-128までである。 キーはTACACS+サーバで構成されたキーと一致しなければならない。

Encrypted/暗号化 - キー文字列が暗号化される際はこのボックスがチェックオンされていること。 この欄はユーザーが読み書き特権を持つ場合のみ表示される。

Connection Timeout/接続タイムアウト - デバイスとTACACS+サーバ間のTCP接続を確立するために許容される最大秒数。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。 .

8.4.5.2 サーバ・コンフィグ

TACACS+
Config | Server Config
TACACS+ Server: Add
IP Address . . .
* = mandatory
Apply

図 : TACACS+ サーバ・コンフィグ

選択基準

TACACS+ Server/TACACS+サーバ - データが表示されるまたは構成されるTACACS+サーバを選択する。 add item/項目を追加するが選択されると、新たなTACACSサーバを構成できる。

構成可能データ

IP Address/IP アドレス - TACACS+サーバのIPアドレスを指定する。
次のIPアドレスを使うことはできない:

- 0.0.0.0
- 255.255.255.255
- 224.xxx.xxx.xxx

- 127.0.0.1

Host Name/ホスト名 - 追加されたサーバのホスト名

Priority/プライオリティ - TACACS+サーバが使用される順序を指定する。 0から65535までの範囲であることが条件である。

Port/ポート -認証ポートを指定する。 0から65535までの範囲であることが条件である。

Key String/キー文字列 - デバイスとTACACS+サーバ間のTACACS+通信のための認証キーと暗号化キーを指定する。 有効な範囲は0から-128までである。 キーはTACACS+サーバで使用される暗号化と一致しなければならない。

Encrypted/暗号化 - キー文字列が暗号化される際はこのボックスがチェックオンされていること。 この欄はユーザーが読み書き特権を持つ場合のみ表示される。

Connection Timeout/接続タイムアウト -デバイスとTACACS+サーバ･タイムアウト間の接続前に経過する時間。 値の範囲は1から30までである。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー･サイクル後、保持されない。

Remove/削除 - 選択されたサーバを構成から削除する。

8.4.6 LDAP

8.4.6.1 構成

	LDAP
Config	
IP Address:*	0 . 0 . 0 . 0
Port(1 to 65535):*	0
Base DN:	
RDN attribute:	
Bind DN without RDN:	
* = mandatory	
	Apply

図 ：LDAPコンフィグ

動作

RDN (相対識別名) の属性が"cn"(共有名)であれば、RDN無しの結合DN(識別名) は"dc=test,dc=com"である。 ユーザー名は"root"、パスワードは"1234"である。結合DNは"cn=root,dc=test,dc=com"、パスワードは"1234"である。 (OU は"組織単位"の略である。. DCは"ドメイン･コンポーネント"の.略である。.)

構成可能データ

IP Address/IPアドレス - LDAPサーバIP、デフォルトは0.0.0.0。

Port/ポート - LDAPサーバTCPポート、デフォルトは389。

ベースDN - 基底識別名、デフォルトは空白文字列である。

RDN attribute/RDN属性 - 結合DNのRDN属性、デフォルトは空白文字列である。

Bind DN without RDN/RDN無し結合DN - 部分的結合DNはRDNを除く、デフォルトは空白文字列である。

コマンドボタン

Apply - LDAPの構成 を入力値で更新する。 パワー･サイクル後、新たな値を保持させるには、保存を実行しなければならない。。

8.4.7　　アクセス制御リスト

8.4.7.1　　IPコンフィグ

IP ACLはパケットに対して順番に一致される規則セットから構成される。 パケットが規則の一致基準に合致すると、指定規則動作(許可か拒否) を行い、追加規則は一致上は確認されない。 このメニューではIP ACLが適用されるインターフェイスを指定し、それがインバウンドかアウトバウンド･トラフィックに適用されるかも指定しなければならない。 IP ACLの規則はIP ACL規則構成メニューを使用して指定し生成される。

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

IP ACL: Create New Standard IP ACL

IP ACL ID (1 to 99) :* 0

* = mandatory

Apply

Table	Current Size / Max Size
ACL	0 / 100

図 ： アクセス制御リストIPコンフィグ

選択基準

IP ACL - プルダウン･メニューから選択する。 新たなIPアクセス制御リストを生成する、または、既存IP ACLの構成を更新することができる。

構成可能データ

IP ACL ID - IP ACL IDはIP標準アクセス･リストでは1から99までの整数、IP拡張アクセス･リストでは100から199までの整数とする。

構成不可能なデータ

Table/テーブル - IP ACの現在数と最大数を表示する。

Current Size/現在のサイズ - IP ACLの現在の数。

Max Size/最大サイズ - IP ACLの最大数。

コマンドボタン

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。. 変更は保存を実行しなければパワー･サイクル後、保持されない。

Delete/削除 - 　現在選択されているIP ACLをIBPの構成から削除する。

8.4.7.2　IPサマリ

図 ： アクセス制御リストIPサマリ

構成不可能なデータ

IP ACL ID - IP ACLの識別子。

Rules/規則 - IP ACLで現在構成されている規則の数。

Direction/方向 - IP ACLの制御をうけるパケット・トラフィックの方向。
方法は次のみとなる:

– インバウンド

Slot/Port(s) / スロット/ポート - IP ACLが適用されるインターフェイス。

コマンドボタン

Refresh/更新 - 画面上のデータを最新状態に更新する。

8.4.7.3　IP規則コンフィグ

IPアクセス制御リストと構成画面を使用して生成されたIP ACLに規則を構成するためにこれらの画面を使用する。 この画面に表示される内容は規則構成の現在段階より異なる。 標準か拡張IP ACLをまず選択して規則を構成する。 規則識別子、'Action'と'Match Every'パラメータを次に指定する。 'Match Every'が偽に設定されると、新画面が表示されここから一致基準を構成する。

図 ： アクセス制御リストIP規則コンフィグ

選択基準

IP ACL ID - プルダウン・メニューで規則を生成または更新するIP ACLを選択する。

Rule/規則 - プルダウン・メニューから既存規則を選択するか、'Create New Rule'(新規則を生成する)を選択する。 ACLのほか新規則を追加するオプション。 新規則は規則の最大数に到達すると生成できない。 規則毎に、パケットは当該規則について真となり指定された規則動作 (許可か拒否) が行われるためには、すべての指定基準と一致しなければならない。

© 2010 富士通テクノロジー・ソリューションズ

構成可能データ

Rule ID/規則ID - 規則を識別するための1から10までの範囲の整数を入力する。 IP ACLは最大10規則を持てる。

Action/動作 - パケットが規則の基準に合致した場合にとられるべき動作を指定する。 選択内容は許可か拒否である。

Logging/ロギング - 'True'に設定されると、このACL規則について (デバイス・リソースの可用性に応じて)ロギングが有効化される。 アクセス・リスト・トラップ・フラッグも有効化された場合、この規則が現在の報告間隔の間に'当たった'回数を示す周期的トラップが生成される。 固定された5分の報告間隔がシステム全体で使用される。 トラップはACL規則の当たり数が現在の間隔で零の場合には発行されない。 この欄は'Deny'動作には見える。

Assign Queue ID/キューIDを割当てる - このIP ACL規則に合致するすべてのパケットを処理するためのハードウェア出口キュー識別子を指定する。 キューIDの有効範囲は0から7までである。 この欄は'Permit'動作には見える。

Mirror Interface/ミラー・インターフェイス - 一致するトラフィックの流れがデバイスによる通常の転送に加えてコピーされる特定の出口インターフェイスを指定する。 この欄はリダイレクト・インターフェイスがすでにACL規則について構成された場合には設定できない。 この欄は'Permit'動作には見える。

Redirect Interface/リダイレクト・インターフェイス - 一致するトラフィックの流れがデバイスによる通常の転送決定を避けて強制される特定の出口インターフェイスを指定する。 この欄はミラー・インターフェイスがすでにACL規則について構成された場合には設定できない。 この欄は'Permit'動作には見える。

Match Every/管理モード - プルダウン・メニューからtrue/真かfalse/偽を選択する。 True/真は、すべてのパケットが選択されたIP ACLと規則に一致し、許可または拒否されることを意味する。 この場合、すべてのパケットが規則に一致するので、他の一致基準を構成するオプションは無い。 規則について特定の一致基準を構成するためには、規則を削除してから再生成するか、'Match Every'を'False'に再構成して他の一致基準が見えるようにする。

Protocol Keyword/プロトコル・キーワード - パケットのIPプロトコルが選択されたIP ACL規則の一致条件であることを指定する。 とりうる値はICMP、 IGMP、 IP、 TCP、及び、UDPである。 'Protocol Keyword'欄または'Protocol Number'欄のいずれかを使用してIPプロトコル値を一致基準に指定できる。

Protocol Number/プロトコル番号 - パケットのIPプロトコルが選択されたIP ACL規則の一致条件であることを指定し、プロトコルを番号で識別する。 プロトコル番号はIANAに割当てられた基準値であり、1から255までの整数として解釈される。'Protocol Number'欄または'Protocol Keyword'欄のいずれかを使用してIPプロトコル値を一致基準に指定できる。

Source IP Address/ソースIPアドレス - ピリオド区画された十進数表記法によりIPアドレスを入力して、選択されたIP ACL規則との一致基準としてパケットのソースIPアドレスと比較する。

Source IP Mask/ソースIPマスク - ピリオド区画された十進数表記法によりIPマスクを指定してソースIPアドレスの値とともに使用する。

Source L4 Port Keyword/ソースL4ポート・キーワード - 選択された拡張IP ACL規則の一致条件としてパケットのソース・レイヤー4ポートを指定する。 これはオプション構成である。 とりうる値はDOMAIN、ECHO、FTP、FTPDATA、HTTP、SMTP、SNMP、TELNET、TFTP、及び、WWWである。 これらの各値は対応するポート番号に変換され、これがポート範囲の開始と終了として使用される。

Source L4 Port Number/ソースL4ポート番号 - 選択された拡張IP ACL規則の一致条件としてパケットのソース・レイヤー4ポートを指定する。 これはオプション構成である。

Destination IP Address/ターゲットIPアドレス - ピリオド区画された十進数表記法によりIPアドレスを入力して、選択された拡張IP ACL規則との一致基準としてパケットのターゲットIPアドレスと比較する。

Destination IP Mask/ターゲットIPマスク - ピリオド区画された十進数表記法によりIPマスクを指定してターゲットIPアドレスの値とともに使用する。

Destination L4 Port Keyword/ターゲットL4ポート・キーワード - 選択された拡張IP ACL規則とのターゲット・レイヤー4ポートの一致基準を指定する。 とりうる値はDOMAIN、ECHO、FTP、FTPDATA、HTTP、SMTP、SNMP、TELNET、TFTP、及び、WWWである。 これらの各値は対応するポート番号に変換され、これがポート範囲の開始と終了として使用される。 これはオプション構成である。

Destination L4 Port Number/ターゲットL4ポート番号 - 選択された拡張IP ACL規則にパケットのターゲット・レイヤー4ポート番号のの一致条件を指定する。 これはオプション構成である。

Service Type/サービス・タイプ - 拡張IP ACL規則にプルダウン・メニューからサービス・タイプの一致条件を選択する。 可能な値はIP DSCP、IP precedence、及び、IP TOSであり、これらはIPヘッダーにある同じサービス・タイプ欄の一致基準を指定する別の方法ではあるが、それぞれ異なるユーザー表記法を用いる。選択後は適切な値を指定できる。

- **IP DSCP Configuration/IP DSCP構成**
  IP DiffServコード・ポイント(DSCP)欄を指定する。 DSCPはIPヘッダー内でサービス・タイプ・オクテットの高い順の 6 ビットとして定義される。 これはオプション構成である。 0 から 63 までの整数を入力する。IP DSCPはドロップダウン・ボックスからDSCPキーワードを 1 個選択して選択される。値を数値を指定して選択する必要がある場合、ドロップダウン・ボックスで'Other'オプションを選択すると、DSCPの数値を入力できるテキストボックスが表示される。
- **IP Precedence Configuration/IPプレシデンス構成**
  パケット内のIPプレシデンス欄はIPヘッダー内でサービス・タイプ・オクテットの高い順の 3 ビットとして定義される。 これはオプション構成である。 0 から 7 の整数を入力する。
- **IP TOS Configuration/IP TOS 構成**
  パケット内のIP TOS 欄はIPヘッダー内でサービス・タイプ・オクテットのすべての 8 ビットとして定義される。 TOSビット値は 00 からFFまでの 16 進数である。 TOSマスク値は 00 からFFまでの 16 進数である。 TOSマスクはパケット内のIP TOS欄と比較するために使用されるTOSビット値内のビット位置を示す。 たとえば、ビット 7 が最も有意である、ビット7および5セットおよびビット 1 クリアを持つIP TOS値を調べるには、TOSビット値 0xA0 とTOSマスク 0xFFを使用する。 これはオプション構成である。

コマンドボタン

Configure/構成 - 選択された規則に対応する一致基準を構成する。

Delete/削除 - 現在選択されている規則を選択されたACLから削除する。 当該変更は保存を実行しないと、パワー・サイクル後、保持されない。

8.4.7.4 MACコンフィグ

図 : アクセス制御リストMACコンフィグ

MAC ACLはパケットに対して順番に一致される規則セットから構成される。 パケットが規則の一致基準に合致すると、指定規則動作(許可か拒否) を行い、追加規則は一致上は確認されない。 このメニューではIP ACLが適用されるインターフェイスを指定し、それがインバウンドかアウトバウンド・トラフィックに適用されるかも指定しなければならない。 IP ACLの規則はIP ACL規則構成メニューを使用して指定し生成される。

選択基準

MAC ACL - 新たなMACアクセス制御リストを生成できる、または、既存のMAC ACL構成を選択に基づいて更新できる。

構成可能データ

MAC ACL名 - 英数字、数字、ダッシュ、アンダースコア、または、空白文字のみからなるMAC ACL名の文字列を指定する。 名前は英数字で始めること。 この欄はACLがすでに生成された場合には現在選択されているMAC ACLの名前を表示する。

構成不可能なデータ

Table/テーブル - MAC ACLの現在数と最大数を表示する。

Current Size/現在のサイズ - MAC ACLの現在の数。

Max Size/最大サイズ - MAC ACLの最大数。

コマンドボタン

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。. 変更は保存を実行しなければパワー・サイクル後、保持されない。

Rename/名前を変更する - 現在選択されているMAC ACLの名前を変える。

Delete/削除 - 現在選択されているMAC ACLをIBPの構成から削除する。

8.4.7.5 MACサマリ

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

MAC ACL Name	Rules	Direction	Slot/Port
abc	0		

Refresh

図 ： アクセス制御リストMACサマリ

構成不可能なデータ

MAC ACL名 - MAC ACL識別子。

Rules/規則 - MAC ACLに現在構成されている規則の数。

Direction/方向 - MAC ACLの制御をうけるパケット・トラフィックの方向。
有効な方向

– インバウンド

Slot/Port(s) / スロット/ポート - MAC ACLが適用されるインターフェイス。

コマンドボタン

Refresh/更新 - 画面上のデータを最新状態に更新する。

8.4.7.6 MAC規則コンフィグ

Access Control Lists

IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config

MAC ACL: abc
Rule: Create New Rule
Rule ID (1 to 10) :*
Action: Deny
Match Every: False
* = mandatory

Apply

図 : アクセス制御リストのMAC規則コンフィグ

選択基準

MAC ACL - 規則を生成または更新するMAC ACLを選択する。

Rule/規則 - 既存の規則を選択するか'Create New Rule'を選択して新規則を追加する。 新規則は規則の最大数に到達すると生成できない。 規則毎に、パケットは当該規則について真となり指定された規則動作 (許可か拒否) が行われるためには、すべての指定基準と一致しなければならない。

構成可能データ

Rule/規則 - 規則を識別するための1から10までの範囲の整数を入力する。

Action/動作 - パケットが規則の基準に合致した場合にとられるべき動作を指定する。 選択内容は許可か拒否である。

Logging/ロギング - 'True'に設定されると、このACL規則について (デバイス・リソースの可用性に応じて) ロギングが有効化される。 アクセス・リスト・トラップ・フラッグも有効化された場合、この規則が現在の報告間隔の間に'当たった'回数を示す周期的トラップが生成される。 固定された5分の報告間隔がシステム全体で使用される。 トラップはACL規則の当たり数が現在の間隔で零の場合には発行されない。 この欄は'Deny'動作には見える。

Assign Queue ID/キューIDを割当てる - このACL規則に合致するすべてのパケットを処理するためのハードウェア出口キュー識別子を指定する。 キューIDの有効範囲は0から7までである。 この欄は'Permit'動作には見える。

Mirror Interface/ミラー・インターフェイス - 一致するトラフィックの流れがデバイスによる通常の転送に加えてコピーされる特定の出口インターフェイスを指定する。 この欄はリダイレクト・インターフェイスがすでにACL規則について構成された場合には設定できない。 この欄は'Permit'動作には見える。

Redirect Interface/リダイレクト・インターフェイス - 一致するトラフィックの流れがデバイスによる通常の転送決定を避けて強制される特定の出口インターフェイスを指定する。 この欄はミラー・インターフェイスがすでにACL規則について構成された場合には設定できない。 この欄は'Permit'動作には見える。

CoS - イーサネット・フレームと比較する802.1pユーザー・プライオリティを指定する。 値の有効範囲は0から7までである。

CoS - イーサネット・フレームと比較する802.1pユーザー・プライオリティを指定する。 値の有効範囲は0から7までである。

ターゲットMAC - イーサネット・フレームと比較するターゲットMACアドレスを指定する。 有効なフォーマットはxx:xx:xx:xx:xx:xxである。

ターゲットMACアドレス01:80:C2:xx:xx:xxを使用してBPDUキーワードを指定できる。

ターゲットMACマスク - イーサネット・フレームとターゲットMACのどのビットを比較するかを指定してターゲットMACアドレス・マスクを指定する。 有効なフォーマットはxx:xx:xx:xx:xx:xxである。

ターゲットMACマスク00:00:00:ff:ff:ffを使用してBPDUキーワードを指定できる。

Ethertype Key/イーサタイプ・キー - イーサネット・フレームと比較するイーサタイプの値を指定する。
有効な値:

- AppleTalk
- ARP
- IBM SNA
- IPv4
- IPv6
- IPX
- MPLS multicast

- MPLS unicast
- NetBIOS
- Novell
- PPPoE
- Reverse ARP
- User Value

Ethertype User Value/イーサータイプ･ユーザー値 - ユーザーが"User Value"をイーサネット･フレームと比較するイーサータイプ･キーとして選択した場合ユーザー定義のカスタマイズ化イーサータイプ値を指定する。 値の有効範囲は0x0600から0xFFFFまでである。

Source MAC/ソースMAC - イーサネット･フレームと比較するソースMACアドレスを指定する。 有効なフォーマットはxx:xx:xx:xx:xx:xxである。

ソースMACマスク - ソースMACのどのビットをイーサネット･フレームと比較するかを指定してソースMACアドレス･マスクを指定する。 有効なフォーマットはxx:xx:xx:xx:xx:xxである。

VLAN - イーサネット･フレームと比較するVLAN IDを指定する。 値の有効範囲は0から4095までである。VLAN範囲またはVLANを構成できる。

Secondary VLAN/2次VLAN - イーサネット･フレームと比較する2次VLAN IDを指定する。 値の有効範囲は0から4095までである。 2次VLAN範囲または2次VLANを構成できる。

Match Every - すべて一致のレイヤー2 MACパケットへの指示を指定する。
有効な値：

- **True/真** - すべてのパケットが選択されたACL規則と一致するとみなされることを意味する。
- **False/偽** - すべてのパケットが選択されたACL規則と一致する必要はないことを意味する。

コマンドボタン

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。変更は保存を実行しなければパワー･サイクル後、保持されない。

Delete/削除 -現在選択されている規則を選択されたACLから削除する。

当該変更は保存を実行しないと、パワー･サイクル後、保持されない。

8.4.7.7 ポート･コンフィグ

Access Control Lists
IP Config | IP Summary | IP Rule Config | MAC Config | MAC Summary | MAC Rule Config | Port Config
Slot/Port: Encl-CB1/0/1
Direction: Inbound
ACL Type:
Sequence Number (1 to 4294967295) :*
* = mandatory
Apply
List of Assigned ACLs

Slot/Port	Direction	ACL Type	ACL Identifier	Sequence Number

図 ： アクセス制御リスト･ポート･コンフィグ

選択基準

Slot/Port / スロット/ポート - ACLマッピングのために利用可能なすべての有効なインターフェイスのリストを指定する。 すべての非ルーティング物理インターフェイスとLAGに参加中のインターフェイスがリストアップされる。

Direction/方向 - ACLのパケット・フィルタリングの方向を指定する。
有効な方向

- インバウンド

ACL Type/ACLタイプ - ACLのタイプを指定する。
有効なACLタイプ

- IP ACL
- MAC ACL

IP ACL - すべてのIP ACLのリストを指定する。 この欄はユーザーが"IP ACL"を"ACL Type"として選択した場合にのみ見える。

MAC ACL - すべてのMAC ACLのリストを指定する。 この欄はユーザーが"MAC ACL"を"ACL Type"として選択した場合にのみ見える。

構成可能データ

Sequence Number/シーケンス番号 - オプションのシーケンス番号を指定してこのインターフェイスと方向にすでに割当てられた他のアクセス・リストに対してこのアクセス・リストの順序を示すことができる。 番号が低いほどプレシデンスは高いことを示す。 シーケンス番号がこのインターフェイスと方向にすでに使用中である場合、指定されたアクセス・リストはそのシーケンス番号を使用して現在付加されたアクセス・リストを置換する。 シーケンス番号がユーザーにより未定義の場合、現在このインターフェイスと方向で使用中の最も高いシーケンス番号より1大きいシーケンス番号が使用される。 許可範囲は1から4294967295である。

構成不可能なデータ

Slot/Port / スロット/ポート -選択されたインターフェイスを表示する。

Direction/方向 - ACLの選択されたパケット・フィルタリングの方向を表示する。

ACL Type/ACLタイプ - 選択されたインターフェイスと方向に割当てられたACLのタイプを表示する。

ACL Identifier/ACL識別子 - 選択されたインターフェイスと方向に割当てられたACLを識別するACL番号(IP ACLの場合) あるいはACL 名(MAC ACLの場合) を表示する。

Sequence Number/シーケンス番号 - 選択されたインターフェイスと方向に割当てられた他のACLに対する指定されたACLの順序を意味するシーケンス番号を表示する。

コマンドボタン

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。. 変更は保存を実行しなければパワー・サイクル後、保持されない。.

Remove/削除 - 現在選択されてい ACLインターフェイスの方向マッピングをIBPの構成から削除する。

8.4.8 IPフィルター

8.4.8.1 構成

管理IPフィルターはIBPの構成変更を許可されたステーションを指定する。 5台までの管理ステーションをIBPの管理用に選択できる。 1台以上の管理ステーションを定義することを選択すると、IPアドレスにより定義された選択ステーションのみウェブ･マネージャ、Telnetｾｯｼｮﾝ、セキュア･シェル (SSH) またはセキュア･ソケット･レイヤー (SSL)でHTTPSの管理特権を許可される。

IP Filter

Config

Admin Mode: Disable

Filter Address 1(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

Filter Address 2(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

Filter Address 3(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

Filter Address 4(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

Filter Address 5(0.0.0.0 = Disable) :* 0 . 0 . 0 . 0

* = mandatory

Apply

図 : IPフィルター･コンフィグ

選択基準

Admin Mode/管理モード - IPフィルターの管理モードを有効化か無効化か選択する。

構成可能データ

フィルター･アドレス 1~5IBPの構成変更を許可されたステーション。

コマンドボタン

Apply - 更新された画面をIBPに設定する。 変更はIBPで反映するが保存を実行しないとパワー･サイクル後、変更は保持されなくなる。

8.4.9 セキュアHTTP

8.4.9.1 構成

図 : セキュアHTTPコンフィグ

構成可能データ

Admin Mode/管理モード - この選択欄はセキュアHTTPの管理モードを有効化か無効化するために使用される。 ウェブページが表示されると現在の構成値が表示される。デフォルト値は無効化である。

TLS Version 1 / TLS バージョン1 -この選択欄はTLSバージョン1.0を有効化か無効化するために使用される。ウェブページが表示されると現在の構成値が表示される。デフォルト値は有効化である。

SSL Version 3 SSL バージョン 3 -この選択欄はSSLバージョン3.0を有効化か無効化するために使用される。ウェブページが表示されると現在の構成値が表示される。デフォルト値は有効化である。

HTTPSポート番号 - この欄はHTTPSポート番号を設定するために使用する。 その値は1～65535の範囲でなければならない。Port44がデフォルト値である。 ウェブページが表示されると現在の構成値が表示される。

HTTPSセッション･ソフト･タイムアウト - この欄はHTTPSセッションの無動作タイムアウトを設定するために使用される。 その値は1～60分の範囲で定める。 デフォルト値は5分である。ウェブページが表示されると現在の構成値が表示される。

HTTPSセッション･ハード･タイムアウト - この欄はHTTPSセッションのハード･タイムアウトを設定するために使用される。 このタイムアウトはセッションの動作レベルには影響されない。 その値は1～168時間の範囲で定める。 デフォルト値は24時間である。ウェブページが表示されると現在の構成値が表示される。

最大HTTPSセッション数 - この欄はHTTPSセッションの最大許容数を設定するために使用される。 その値は0～16回の範囲で定める。 デフォルト値は16である。ウェブページが表示されると現在の構成値が表示される。

コマンドボタン

Apply - 更新された画面をIBPに送る。変パワー･サイクル後、新たな値を保持させるには、保存を実行しなければならない。

Download Certificates/ダウンロード証明書 - SSL証明書のダウンロード用ファイル転送頁へのリンクである。 SSL証明書ファイルをダウンロードするにはSSLは管理上無効化されなければならない。

8.4.10　セキュア･シェル

8.4.10.1　構成

Secure Shell

Config

Admin Mode: Disable

SSH Version 1: Enable

SSH Version 2: Enable

SSH Connections Currently in Use: 0

Maximum number of SSH Sessions Allowed: 5

SSH Session Timeout (minutes) (1 to 160) :* 5

* = mandatory

Download Host Keys　Apply

図 ： セキュア･シェル･コンフィグ

構成可能データ

Admin Mode/管理モード - この選択欄はSSHの管理モードを有効化か無効化するために使用される。 ウェブページが表示されると現在の構成値が表示される。デフォルト値は無効化である。

SSH Version 1 / SSH バージョン 1 -この選択欄はSSHにプロトコル･レベル1を有効化か無効化するために使用される。 ウェブページが表示されると現在の構成値が表示される。デフォルト値は有効化である。

SSH Version 2 / SSH バージョン 2 - この選択欄はSSHにプロトコル･レベル2を有効化か無効化するために使用される。ウェブページが表示されると現在の構成値が表示される。デフォルト値は有効化である。

Maximum Number of SSH Sessions Allowed/許可された最大SSHセッション数 - この選択欄はIBPで許可される最大インバウンドSSHセッション数を構成するために使用される。ウェブページが表示されると現在の構成値が表示される。この欄で許容される値の範囲は0から5までである。

SSH Session Timeout (Minutes)/SSHセッション･タイムアウト- このテキスト欄はIBPへのインバウンドSSHセッションに無動作タイムアウト値を構成するために使用される。 許容される値の範囲は0から160分までである。

構成不可能なデータ

SSH Connections in Use/使用中のSSH接続数 - システムで現在使用中のSSH接続数を表示する。

コマンドボタン

Apply - 更新された画面をIBPに送る。変パワー･サイクル後、新たな値を保持させるには、保存を実行しなければばならない。

Download Host Keys/ホストキーをダウンロードする - ホストキーのダウンロード用ファイル転送頁へのリンクである。SSHキーファイルをダウンロードするにはSSHは管理者により無効化されなければならず、アクティブなSSHセッションがあってはならない。

© 2010 富士通テクノロジー･ソリューションズ

8.4.11 サービス妨害攻撃

8.4.11.1 構成

Denial-of-Service

Config

SIP=DIP: Disable
First Fragment: Disable
TCP Fragment: Disable
TCP Flag: Disable
L4 Port: Disable
ICMP: Disable
Max ICMP Size (0 to 1023):* 512
Max ICMPv6 Size (0 to 1023):* 512
* = mandatory

Apply

図 : サービス妨害攻撃コンフィグ

構成可能データ

SIP=DIP - プルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。 SIP=DIP DoS予防を有効化するとIBPは、ターゲットIPアドレスと同じソースIPアドレスがあるパケットを落とす。 工場側デフォルトは無効化されている。

第1フラグメントプルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。 第1フラグメントDoS防止を有効化するとIBPは構成された最小TCPヘッダー・サイズより小さいTCPヘッダーをもつパケットを落とす。工場側デフォルトは無効化されている。

Min TCP Hdr Size/最小TCPヘッダー・サイズ - 許可される最小TCPヘッダー・サイズを指定する。 第1フラグメントDoS防止を有効化すると、IBPは構成された最小TCPヘッダー・サイズより小さいTCPヘッダーをもつパケットを落とす。 工場側デフォルトは無効化されている。*(注記: この属性はスタック可能イーサネット・コネクション・ブレードには提供される)*

TCP Fragment/TCP フラグメント プルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。 第1フラグメントDoS防止を有効化するとIBPは構成された最小TCPヘッダー・サイズより小さいTCPヘッダーをもつパケットを落とす。工場側デフォルトは無効化されている。

TCP Flag/TCPフラッグプルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。 TCPフラッグDoS防止を有効化するとIBPは、1024より小さいTCPフラッグSYNセットとTCPソース・ポートまたは0に設定されたTCP制御フラッグ、0に設定されたTCPシーケンス番号またはTCPフラッグFIN、URG、PSHセット及び0に設定されたTCPシーケンス番号またはTCPフラッグSYNセットとFINセットの両方を持つパケットを落とす。 工場側デフォルトは無効化されている。

L4 Port/L4ポート - プルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。 L4ポートDoS防止を有効化するとIBPはTCP/UDPターゲット・ポートに等しいTCP/UDPソース・ポートをもつパケットを落とす。 工場側デフォルトは無効化されている。

ICMP プルダウン入力欄の該当行を選択してこのオプションを有効化または無効化する。 ICMP DoS防止を有効化するとIBPは、タイプがECHO_REQ (ping)に設定され構成されたICMPパケット・サイズより大きいサイズのICMKPパケットを落とす。 工場側デフォルトは無効化されている。

Max ICMP Pkt Size/最大ICMPパケット・サイズ - 許可される最大のICMPパケット・サイズを指定する。 ICMP DoSが有効化されている場合、IBPはこの構成された最大ICMPパケット・サイズより大きいサイズのICMP pingパケットを落とす。 工場側デフォルトは無効化されている。

Max ICMPv6 Pkt Size/最大ICMPv6 パケット・サイズ - 許可される最大のICMPv6 パケット・サイズを指定する。 ICMP DoSが有効化されている場合、IBPはこの構成された最大ICMPv6 パケット・サイズより大きいサイズのICMPv6 pingパケットを落とす。工場側デフォルトは無効化されている。

© 2010 富士通テクノロジー・ソリューションズ

コマンドボタン

Apply - IBP を画面の値で更新する。 IBPにパワー･サイクル後に保持させるには保存を実行する。

© 2010 富士通テクノロジー･ソリューションズ

8.5 QoS Menu

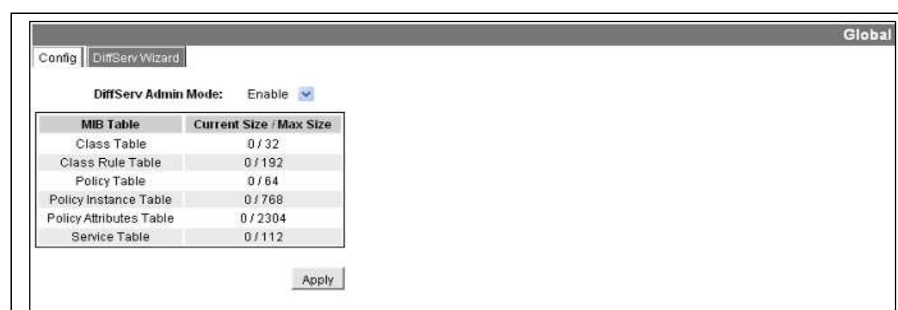
8.5.1 差別化サービス

8.5.1.1 グローバル･コンフィグ

パケットは定義された基準に基づいてフィルターされ、処理される。 フィルタリング基準はクラスにより定義される。 処理はポリシーの属性により定義される。 ポリシー属性はクラス毎のインスタンスに基づいて定義され、一致時には当該属性が適用される

構成プロセスはクラスに1個またはそれ以上の一致基準を定義することから開始する。 次に1個またはそれ以上のクラスがポリシーに追加される。 次にポリシーがインターフェイスに追加される。

パケット処理はパケットについて一致基準をテストすることから開始する。 'all'クラス･タイプのオプションはクラス内の各一致基準はパケットがそのクラスと一致するためにはtrue/真と評定されることが必要であると定義する。 'any'クラス･タイプのオプションは少なくとも1個の一致基準はパケットがそのクラスと一致するためにはtrue/真と評定されることが必要であると定義する。 クラスはポリシーに追加された順にテストされる。 ポリシーはポリシー内でクラス一致が発見されたときにパケットに追加される。



MIB Table	Current Size / Max Size
Class Table	0 / 32
Class Rule Table	0 / 192
Policy Table	0 / 64
Policy Instance Table	0 / 768
Policy Attributes Table	0 / 2304
Service Table	0 / 112

図 : DiffServのグローバル･コンフィグ

選択基準

DiffServ Admin Mode/DiffServの管理モード - このモードのオプションをリストし、そこから1個を選択できる。 デフォルト値は'enable'/有効化である。 無効化されている間は、DiffServの構成は保存されていれば保持され、変更できるが、アクティブ化はできない。 有効化されると、DiffServサービスはアクティブ化される。

構成不可能なデータ

Class table/クラス･テーブル - IBPに許可された総数のうち構成されたDiffServクラスの数を表示する。

Class Rule table/クラス規則テーブル - IBPに許可された総数のうち構成されたクラス規則の数を表示する。

Policy table/ポリシー･テーブル - IBPに許可された総数のうち構成されたポリシーの数を表示する。

Policy Instance table/ポリシー･インスタンス･テーブル - IBPに許可された総数のうち構成されたポリシー･クラス･インスタンスの数を表示する。

Policy Attributes table/ポリシー属性テーブル - IBPに許可された総数のうち(ポリシー･クラス･インスタンツに付加された)構成されたポリシー属性の数を表示する。

Service table/サービス･テーブル - IBPに許可された総数のうち(指定されたインターフェイスでポリシーに付加された)構成されたサービスの数を表示する。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。

8.5.1.2 DiffServウィザード

DiffServウィザードは、トラフィック・クラスの生成、ポリシーへのこのトラフィック・クラスの追加、次にDiffServウィザード頁で選択されたポートへのポリシーの追加によりIBPでDiffServを有効化する。 DiffServウィザードが行うこと:

- DiffServクラスを生成し、入ってくるトラフィックがクラス・メンバーとなるための要件に合致するかを決めるフィルターとして使用される一致基準を定義する。
- 次のようにトラフィック・タイプに基づいてDiffServクラスの一致基準を設定する:

– VOIP - UDPプロトコルに一致基準を設定する。

– HTTP - sets match criteria to HTTP ターゲット・ポートに一致基準を設定する。

– FTP - sets match criteria to FTP ターゲット・ポートに一致基準を設定する。

– Telnet - sets match criteria to Telnet ターゲット・ポートに一致基準を設定する。

– Every - すべてのトラフィックに一致基準を設定する。

- DiffServポリシーを生成し、DiffServポリシーを生成されたDiffServクラスに追加する。
- ポリシー化がYES/有りに設定された場合、DiffServポリシー・スタイルはSimple/簡易に設定される。 クラス一致基準に合致したトラフィックはアウトバウンド・プライオリティの選択に従い処理される。 アウトバウンド・プライオリティは次のように、合致したトラフィックの処理を構成する:

– High - markdscp efにポリシー化動作を設定する。

– Med - markdscp af31 にポリシー化動作を設定する。

– Low - 送信するポリシー化動作を設定する。

- ポリシー化がNO/無しに設定された場合、すべてのトラフィックが次に指定するようにマークされる:

– High - ipdscp efのポリシー・マークを設定する。

– Med - ipdscp af31 のポリシー・マークを設定する。

– Low - ipdscp beのポリシー・マークを設定する。

- 選択された各ポートは生成されたポリシーに追加される。

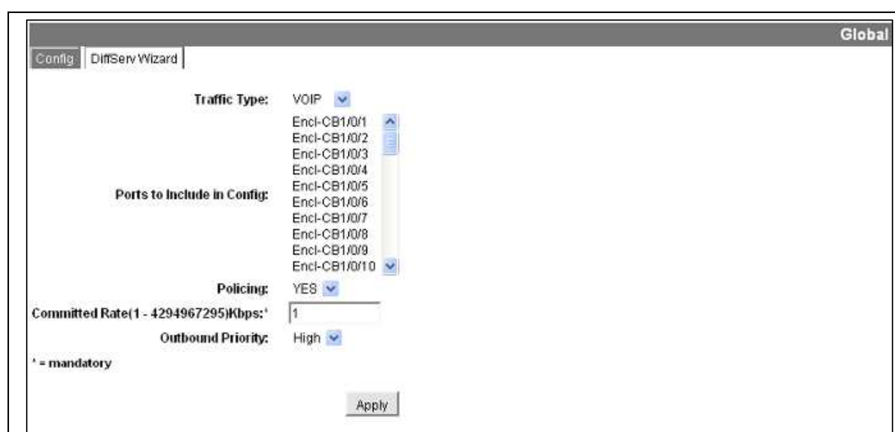


図 : 差別化サービス・ウィザード

選択基準

Traffic Type/トラフィック･タイプ - トラフィック･タイプはDiffServ クラスを定義するために使用される。 トラフィック･タイプのオプション： VOIP、 HTTP、FTP、Telnet、Every。

ポリシー化 - ポリシー化を有効化するとポリシー設定をDiffServポリシーに追加し、ポリシー化率が適用される。

Outbound Priority/アウトバウンド･プライオリティ - ポリシー化を有効化するとアウトバウンド･プライオリティはポリシー化に合致するアクションをタイプを定義し、ここに： Highは動作をmarkdscp efに設定し、Medは動作をmarkdscp af31に設定し、Lowは動作をsendに設定する。 ポリシー化を無効化するとアウトバウンド･プライオリティはポリシーを定義する、ここに： Highはポリシーをipdscp efマークに設定し、 Medはポリシーをipdscp af31マークに設定し、 Lowポリシーをipdscp beマークに設定する。

構成可能データ

コンフィグに含めるポート - DiffServポリシーをサポートするために構成できるポートをリストする。 DiffServポリシーは選択されたポートに追加される。

Committed Rate/占有率 - ポリシー化を有効化すると占有率がポリs-に適用され、ポリシー化動作はconform/一致に設定される。 ポリシー化を無効化すると占有率は適用されず、ポリシーはmarkdscpに設定される。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー･サイクル後、保持されない。.

8.5.1.3 クラス･コンフィグ

Class Config | Class Summary

Class Selector: Create
Class Name:*
Class Type:
* = mandatory

Apply | Cancel

図 : 差別化サービスのクラス･コンフィグ

選択基準

Class Selector/クラス･セレクタ - 新クラスを生成するオプションとともに、これはすべての既存のDiffServｸﾗｽ名をリストし、ここから1個選択できる。 この画面の内容はこの欄での選択に応じて変る。 既存クラスが選択された場合画面は構成されたクラスを表示する。 '--create--'が選択された場合、新ｸﾗｽ生成が便利にできる別の画面が表示される。 デフォルトは最初のクラスが生成された状態である。 クラスが存在しない場合、デフォルトは'--create--'/生成するである。

Class Type/クラス･タイプ - プラットフォームでサポートされるすべてのDiffServクラスをリストしここから1個を選択できる。 オプション:

- All

新ｸﾗｽが生成されるときのみ、この欄は選択欄である。 クラスの生成後、これは構成されたクラス･タイプを表示する構成不可の欄に変る。

Class Match Selector/クラス一致セレクタ - これはすべての一致基準をリストし、ここから1個を選択して指定されたクラスに追加できる。 一致基準'Any'は、すべてのパケットが指定されたクラスに一致すると見なされ、追加の入力情報は不要であることを意味する。 このドロップダウン･リストの内容は'Reference Class'の一致基準の選択に応じて指定されたクラスについて変る。

- 指定されたクラスが別のクラスを参照しない場合、'Reference Class'の一致基準はドロップダウン一致基準リストに含まれる。 クラスへの参照は'Reference Class'を選択すると確立でき、これは'Add Match Criteria'ボタンを表示させる。
- 指定されたクラスが別のクラスを参照する場合、'Reference Class'の一致基準はドロップダウン一致基準リストに含まれない。 これにより、指定されたクラスが同じタイプの別の1クラスを参照できるのでユーザーが別のクラス参照を追加するのを防ぐ。 さらに、画面には現在のクラス参照を削除するために呼び出される'Remove Class Reference'ボタンが表示される。

構成可能データ

Class Name/クラス名 - これは一意にクラスを識別する1から31文字までの大文字･小文字を区別する英数字文字列である。 'default'というクラス名は予約されており、使用できない。

構成不可能なデータ

Class Type/クラス･タイプ - 新たなクラスが生成されたときのみ、構成されたクラスにタイプを表示する。 この欄は選択欄である。 クラスの生成後はこの欄は構成不可欄となる。

Match Criteria/一致基準 - 指定されたクラスの構成された一致基準を表示する。

Values/値 - 構成された一致基準の値を表示する。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー･サイクル後、保持されない。 .

Cancel/取消 - 現在選択されているフィルターを取り消す。

Delete/削除 - 現在選択されているフィルターを削除する

Rename/名前を変更する - 指定されたクラスの名前を変えることができる。

Add Match Criteria/一致基準を追加する - このボタンが呼び出される度に1個のみの一致基準を指定できる。 選択された一致基準に基づいて、個々の一致基準画面が表示され値を構成できる。

i

一致基準はクラスから削除できない。 一致基準を削除するためにはクラスを削除しなければならない。

Remove Class Reference/クラス参照を削除する - 指定されたクラスが別のクラスを参照する場合のみこのボタンが画面に現れる。 指定されたクラスの現在のクラス参照がこのボタンを呼び出すと削除される。

© 2010 富士通テクノロジー・ソリューションズ

8.5.1.4 クラス･サマリ

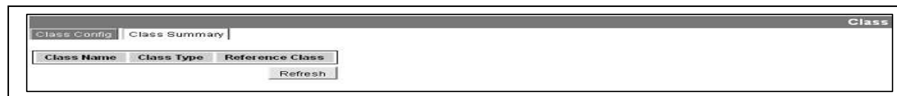


図 ： 差別化サービスのクラス･サマリ

構成不可能なデータ

Class Name/クラス名 - 構成されたDiffServクラスの名前を表示する。

Class Type/クラス･タイプ - 構成されたクラスのタイプを表示する。クラス･タイプはプラットフォームに依存する。

Reference Class/参照クラス - 同じタイプの指定されたクラスに参照されるそ

- **のタイプに構成されたクラスの名前を表示する。**

コマンドボタン

Refresh/更新 - 現在選択されているフィルターを更新する。

8.5.1.5　ポリシー・コンフィグ

Policy	
Config / Summary / Class Definition / Attribute Summary	
Policy Selector:	Create
Policy Name:*	
Policy Type:	In
* = mandatory	
	Apply

図 ： 差別化サービスのポリシー・コンフィグ

選択基準

Policy Selector/ポリシー・セレクタ - 新クラスを生成するオプションとともに、これはすべての既存のDiffServポリシー名をリストし、ここから1個選択できる。 この画面の内容はこの欄での選択に応じて変る。既存折シーが選択されると、画面はそのDiffServポリシーのメンバー・クラスを表示する。 'create'が選択された場合、新ポリシーが便利に生成できる別の画面が表示される。 デフォルトは'create'/生成するである。

Policy Type/ポリシー・タイプ - *In* の意味は当該タイプがインバウンド・トラフィック方向に固有であることを示す。 新ポリシーが生成されるときのみ、この欄は選択欄である。 ポリシーの生成後、これは構成されたポリシー・タイプを表示する構成不可の欄に変る。

Available Class List/利用可能なクラスのリスト - 既存すべてのDiffServクラス名をリストし、ここから1個選択できる。 この欄は新たなポリシー・クラス・インスタンスが生成されるときのみ選択欄である。 ポリシー・クラス・インスタンスの生成後はこの欄は構成不可欄となる。

Member Class List/メンバー・クラス・リスト - 指定されたポリシーのメンバーとして現在定義されている既存すべてのDiffServクラスをリストし、ここから1個選択できる。 このリストは新たなクラスがポリシーに追加または削除されると自動的に更新される。 この欄は既存のポリシー・クラス・インスタンスが削除されるときのみ選択欄である。 ポリシー・クラス・インスタンスの削除後はこの欄は構成不可欄となる。

構成可能データ

Policy Name/ポリシー名 - これは一意にポリシーを識別する1から31文字までの大文字・小文字を区別する英数字文字列である。

構成不可能なデータ

Policy Type/ポリシー・タイプ - *In* の意味は当該タイプがインバウンド・トラフィック方向に固有であることを示す。 新ポリシーが生成されるときのみ、この欄は選択欄である。 ポリシーの生成後、これは構成されたポリシー・タイプを表示する構成不可の欄に変る。

Member Class List/メンバー・クラス・リスト - 選択された DiffServ ポリシーのメンバー・クラスをすべて表示する。 新たなクラスがポリシーに追加または削除されると自動的に更新される。 この欄は既存のポリシー・クラス・インスタンスが削除されるときのみ選択欄である。 ポリシー・クラス・インスタンスの削除後はこの欄は構成不可欄となる。

Available Class List/利用可能なクラス・リスト - 指定されたポリシーのメンバー・クラスをすべて表示する。 新たなクラスがポリシーに追加または削除されると自動的に更新される。 . この欄は新ポリシー・クラス・インスタンスが生成されるときのみ選択欄である。 ポリシー・クラス・インスタンスの生成後はこの欄は構成不可欄となる。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー・サイクル後、保持されない。

© 2010 富士通テクノロジー・ソリューションズ

Delete/削除 - 現在選択されているフィルターを削除する.

Rename/名前を変更する - 指定されたポリシーの名前を変えることができる。

Add Selected Class/選択されたクラスを追加する - ポリシーを指定されたクラスに付加してポリシー･クラス･インスタンスを生成する。

Remove Selected Class/選択されたクラスを削除する - ポリシーを指定されたクラスから切り離してポリシー･クラス･インスタンスを削除する。

© 2010 富士通テクノロジー･ソリューションズ

8.5.1.6　　ポリシー・サマリ

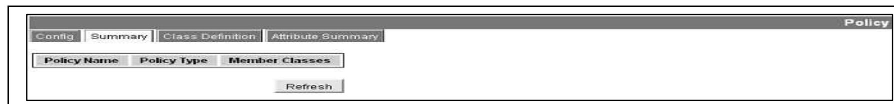


図 ： 差別化サービスのポリシー・サマリ

構成不可能なデータ

Policy Name/ポリシー名 - DiffServポリシーの名前を表示する。

Policy Type/ポリシー・タイプ - ポリシー・タイプをIn (インバウンド) として表示する。

Member Classes/メンバー・クラス - ポリシー内の各クラス・インスタンsぬの名前を表示する。

コマンドボタン

Refresh/更新 - 現在選択されているフィルターを更新する。

8.5.1.7　ポリシー・クラス定義

Policy
Config | Summary | Class Definition | Attribute Summary

Policy Selector: None
Policy Type:
Member Class List: No Member Classes
Policy Attribute Selector: No Member Classes

図 ： 差別化サービス・ポリシー・クラスの定義

選択基準

Policy Selector/ポリシー・セレクタ - 既存すべてのDiffServポリシー名をリストし、ここから1個選択できる。

Member Class List/メンバー・クラス・リスト - 指定されたポリシーのメンバーとして現在定義されている既存すべてのDiffServクラスをリストし、ここから1個選択できる。 このリストは新たなクラスがポリシーに追加または削除されると自動的に更新される。 .

Policy Attribute Selector/ポリシー属性セレクタ - このタイプのポリシーでサポートされるすべての属性をリストし、ここから1個選択できる。

構成不可能なデータ

Policy Type/ポリシー・タイプ - 構成されたポリシー・タイプを表示する。

コマンドボタン

Configure Selected Attribute/選択された属性を構成する - 1個のみの構成基準をこのボタンを呼び出す度に指定できる。 選択された構成基準に基づいて、個々の構成画面が提供される。

8.5.1.8　　ポリシー属性サマリ

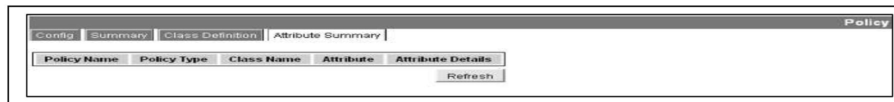


図 : 差別化サービスのポリシー属性サマリ

構成不可能なデータ

Policy Name/ポリシー名 - 指定されたDiffServポリシーの名前を表示する。

Policy Type/ポリシー･タイプ - 指定されたポリシー･タイプをIn (インバウンド) として表示する。

Class Name/クラス名 - ポリシーが付加されたDiffServクラスの名前を表示する。

Attribute/属性 - ポリシー･クラス･インスタンスに付加された属性を表示する。

Attribute Details/属性詳細 - 付加された属性の構成された値を表示する。

コマンドボタン

Refresh/更新 - 表示されたデータを更新する。

8.5.1.9　サービス･コンフィグ

Service
Config | Summary | Statistics | Detailed Statistics
Slot/Port: Encl-CB1/0/1
Policy In: None
Apply

図 ： 差別化サービスのサービス･コンフィグ

選択基準

Slot/Port / スロット/ポート -インターフェイスを一意に指定するスロット/ポートを選択する。 システムの有効なすべてのスロット番号とポート番号の組合わせをリストする。 読み･書き特権ユーザーではリストに'All'と表示されている場合、すべてのインターフェイスを指定するために選択できる。

Direction/方向 - このサービス･インターフェイスのトラフィック方向を選択する。 この選択はスロット/ポートが'All'に指定された場合には読み･書き特権ユーザーのみ利用できる。

構成可能データ

Policy In/Inのポリシー - 'In'タイプのすべてのポリシー名をリストし、ここから1個選択できる。 'none'/無しが選択された場合、当該ポリシーをこの方向のインターフェイスから切り離す。 インバウンド･サービス･ポリシーの付加がプラットフォームによりサポートされていない読み･書き特権ユーザーにはこの欄は見えない。

構成不可能なデータ

この情報はスロット/ポートが'All'に指定された場合のみ表示される。

Slot/Port / スロット/ポート -インターフェイスを一意に指定するスロット/ポートを表示する。

Direction/方向 - このサービス･インターフェイスのトラフィック方向がインバウンドであることを表示する。

Oper. Status / 動作 状態 - このサービス･インターフェイスの動作状態、アップかダウンかを表示する。

Policy Name/ポリシー名 - 付加されたポリシーの名前を表示する。

コマンドボタン

Apply - IBPに更新された画面を送り、IBPに変更を有効化するが、変更は保存を実行しないと、パワー･サイクル後、保持されない。

8.5.1.10　サービス･サマリ

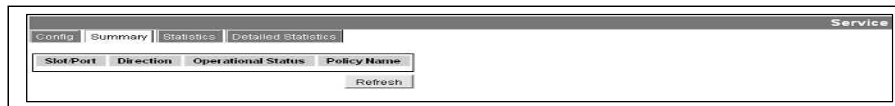


図 : 差別化サービスのサービス･サマリ

構成不可能なデータ

Slot/Port / スロット/ポート - インターフェイスを一意に指定するスロット/ポートを表示する。

Direction/方向 - このサービス･インターフェイスのトラフィック方向がインバウンドであることを表示する。

Oper. Status / 動作 状態 - このサービス･インターフェイスの動作状態、アップかダウンかを表示する。

Policy Name/ポリシー名 - 付加されたポリシーの名前を表示する。

コマンドボタン

Refresh/更新 - 表示されたデータを更新する。

© 2010 富士通テクノロジー･ソリューションズ

8.5.1.11　サービス統計

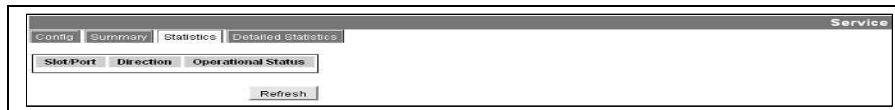


図 : 差別化サービスのサービス統計

この画面はDiffServポリシーがインバウンド･トラフィック方向で付加されたシステム内すべてのインターフェイスについてテーブル形式でサービス･レベル統計情報を表示する。 'Counter Mode Selector'(カウンター･モード･セレクタ)を用いてカウンター表示モードをオクテットまたはパケットに指定する。

構成不可能なデータ

Slot/Port / スロット/ポート - インターフェイスを一意に指定するスロット/ポートを表示する。

Direction/方向 - このサービス･インターフェイスのトラフィック方向がインバウンドであることを表示する。

Operational Status/動作状態 - このサービス･インターフェイスの動作状態、アップかダウンかを表示する。

コマンドボタン

Refresh/更新 - 表示されたデータを更新する。

8.5.1.12　サービス詳細統計

この画面は、インターフェイスと方向により指定される、ポリシーのクラスごとの統計情報を表示する。 'Member Classes'ドロップダウン・リストは指定されたインターフェイスと方向つまり付加されたポリシー (該当する場合) に基づいて内容が決まる。 メンバー・クラス名をハイライトすると指定されたインターフェイスと方向についてのポリシー・クラス・インスタンスの統計情報が表示される。

Service
Config　Summary　Statistics　Detailed Statistics
Slot/Port: None
Direction: None
Policy Name :
Operational Status:
Member Classes: None
Refresh

図 : 差別化サービスのサービス詳細統計

選択基準

Slot/Port / スロット/ポート -現在インバウンド方向に付加されているDiffServポリシーをもつシステム内の有効なすべてのスロット番号とポート番号の組合わせをリストする。

Direction/方向 -インターフェイスのトラフィック方向がインバウンドであるものをリストする。DiffServポリシーが現在付加されている方向のみ表示される。

Member Classes/メンバー・クラス -選択されたポリシー名のメンバーに現在定義されているすべてのDiffServクラスをリストする。　統計を表示するためには1回に1子のメンバー・クラス名を選ぶ。 選択されたポリシーと関連付けられたクラスが無い場合、リストには何も含まれない。

構成不可能なデータ

Policy Name/ポリシー名 - 指定されたインターフェイスと方向に現在付加されているポリシーの名前。

Operational Status/動作状態 -指定されたインターフェイスと方向に現在付加されているポリシーの動作状態。 値はUpかDownである。

コマンドボタン

Refresh/更新 - 表示されたデータを更新する。

8.5.2 CoS

8.5.2.1 信頼モード

Class of Service

Trust Mode | IP DSCP Mapping | Priority Mapping | Interface | Interface Queue | Interface Queue Status

Slot/Port: Encl-CB1/0/1

Interface Trust Mode: trust dot1p

test

Apply | Restore Defaults

Current 802.1p Priority Mapping	
802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

*In order to map Traffic class with dot1p go to QoS-->Class of service-->Priority Mapping

図：CoS信頼モード

選択基準

Slot/Port / スロット/ポート -すべてのCoS構成可能なインターフェイスを指定する。 ”Global"オプションは直前のグローバル構成の設定を表す。 インターフェイス毎にはオーバーライドされていることがある。

Interface Trust Mode/インターフェイストランスモード - 入口で特定のパケットのマーキングを信頼するかを指定する。
インターフェイス信頼モードは次のうち1個のみの値をとりうる；

– untrusted/アントランス
– trust dot1p/dot1pトランス
– trust ip-dscp/ip-dscpトランス

デフォルト値はtrust dot1pである。

構成不可能なデータ

Untrusted Traffic Class/信頼されないトラフィック・クラス - 'untrusted'モードにある場合すべてのトラフィックが向かうトラフィック・クラス(すなわち、キュー) を表示する。 有効な範囲は0から7である。

Non-IP Traffic Class/非IPトラフィック・クラス - 'trust ip-precedence'または'trust ip-dscp'モードにある場合、すべての非IPトラフィックが向かうトラフィック・クラス(すなわち、キュー) を表示する。 有効な範囲は0から7である。

Current 802.1p Priority Mapping/現在の802.1pプライオリティ・マッピング - 現在の802.1pプライオリティ・マッピングの構成を表示する。

コマンドボタン

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。. 変更は保存を実行しなければパワー・サイクル後、保持されない。.

Restore Defaults/デフォルトを復元する - デフォルト設定に戻す。

8.5.2.2　　IP DSCPマッピング

Class of Service

Trust Mode | IP DSCP Mapping | Priority Mapping | Interface | Interface Queue | Interface Queue Status

Slot/Port: Global

IP DSCP Value	Traffic Class
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	1

図 : CoS IP DSCPマッピング

選択基準

Slot/Port / スロット/ポート - すべてのCoS構成可能なインターフェイスを指定する。 "Global"オプションは直前のグローバル構成の設定を表す。

構成可能データ

IP DSCP Traffic Class/IP DSCPトラフィック・クラス - どの内部トラフィック・クラスが対応する IP DSCP値にマップされるかを指定する。 有効な範囲は0から7である。

構成不可能なデータ

IP DSCP Value/IP DSCP値 IP DiffServコード・ポイント(DSCP)値を指定する。

コマンドボタン

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。. 変更は保存を実行しなければパワー・サイクル後、保持されない。.

Restore Defaults/デフォルトを復元する - デフォルト設定に戻す。

8.5.2.3　プライオリティ・マッピング

Class of Service

Trust Mode | IP DSCP Mapping | Priority Mapping | Interface | Interface Queue | Interface Queue Status

Slot/Port: All

802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Apply　Restore Defaults

図 ：CoSプライオリティ・マッピング

選択基準

Slot/Port / スロット/ポート -データを表示または構成する物理インターフェイスを選択する。 すべてのポートのパラメータを同じ値に設定するには'All'を選択する。

構成可能データ

Traffic Class/トラフィック・クラス - 対応する802.1pプライオリティをどの内部トラフィック・クラスがマップするかを指定する。

構成不可能なデータ

802.1p Priority/802.1pプライオリティ - マップされる802.1pプライオリティを表示する。

コマンドボタン

Apply - IBP を画面の値で更新する。IBPにパワー・サイクル後、設定を保持させるには、保存を実行しなければならない。. .。

Restore Defaults/デフォルトを復元する - デフォルト設定に戻す。

© 2010 富士通テクノロジー・ソリューションズ

8.5.2.4 インターフェイス

図 : CoSインターフェイス･コンフィグ

選択基準

Slot/Port / スロット/ポート - すべてのCoS構成可能なインターフェイスを指定する。 ”Global”オプションは直前のグローバル構成の設定を表す。 インターフェイス毎にはオーバーライドされていることがある。

構成可能データ

Interface Shaping Rate/インターフェイス･シェイピング速度 - アウトバウンド送信速度を決めるために通常使用する最大許容帯域を指定する。 この値はキュー毎の最大帯域構成とは無関係に制御される。 効果的に2次レベルのシェーピングとなっている。 デフォルト値は0である。値の範囲は5ずつ増える0から100である。 値0とは最大速度は無制限であることを意味する。

コマンドボタン

Restore Defaults/デフォルトを復元する - デフォルト設定に戻す。

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。. 変更は保存を実行しなければパワー･サイクル後、保持されない。.

8.5.2.5　インターフェイス･キュー

図 ：CoSインターフェイス･キュー･コンフィグ

選択基準

Slot/Port / スロット/ポート - すべてのCoS構成可能なインターフェイスを指定する。 "Global"オプションは直前のグローバル構成の設定を表す。 インターフェイス毎にはオーバーライドされていることがある。

Queue ID/キューID - インターフェイス毎（プラットフォーム･ベースで）に利用可能なすべてのキューを指定する。

Scheduler Type/スケジューラ･タイプ - このキューに使用されるスケジューリングの種類を指定する。
スケジューラ･タイプは次のうち1個のみである：

- strict
- weighted

デフォルト値はweightedである。

Queue Management Type/キュー管理タイプ - このインターフェイスでキューに使用されるキュー長管理方法です。 これはデバイスがキュー毎に独立的設定をサポートする場合のみ使用される。
キュー管理タイプは次のうち1個のみである：

- taildrop

デフォルト値はtaildropである。

構成可能データ

Minimum Bandwidth Allocated/最小割当て帯域 - インターフェイス内すべてのキューに個々の最小帯域値の合計を指定する。 合計値は定義された最大値100を超過できない。 選択されたインターフェイスにキューの最小帯域を構成する間にこの値が考慮される。

Minimum Bandwidth/最小帯域 - このキューに割当てられる最小保証帯域を指定する。 この値を対応する最大帯域より高く設定すると自動的に最大帯域の値が同じ値に増加する。 デフォルト値は0である。値の範囲は5ずつ増える0から100である。 値0は保証最小値がないことを意味する。 選択されたインターフェイスにあるすべてのキューの個別最小帯域の合計は定義された最大値100を超過できない。

コマンドボタン

Restore Defaults for All Queues/すべてのキューにデフォルトを復元する - 選択されたインターフェイスのすべてのキュー設定をデフォルト値に戻す。

Apply - 更新された構成をIBP設定する。 構成変更は直ちに反映される。. 変更は保存を実行しなければパワー･サイクル後、保持されない。

© 2010 富士通テクノロジー･ソリューションズ

8.5.2.6　　インターフェイス・キュー・ステータス

Class of Service

Trust Mode | IP DSCP Mapping | Priority Mapping | Interface | Interface Queue | Interface Queue Status

Slot/Port: Encl-CB1/0/1

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
0	0	weighted	taildrop
1	0	weighted	taildrop
2	0	weighted	taildrop
3	0	weighted	taildrop
4	0	weighted	taildrop
5	0	weighted	taildrop
6	0	weighted	taildrop
7	0	weighted	taildrop

図 ：CoSインターフェイス・キュー・ステータス

選択基準

Slot/Port / スロット/ポート - すべてのCoS構成可能なインターフェイスを指定する。 "Global"オプションは直前のグローバル構成の設定を表す。 インターフェイス毎にはオーバーライドされていることがある。

構成不可能なデータ

Queue ID/キューID - キューIDを指定する。

Minimum Bandwidth/最小帯域 - このキューに割当てられる最小保証帯域を指定する。 値0は保証最小値がないことを意味する。 選択されたインターフェイスにあるすべてのキューの個別最小帯域の合計は定義された最大値100を超過できない。

Scheduler Type/スケジューラ・タイプ - このキューに使用されるスケジューリングの種類を指定する。
スケジューラ・タイプは次のうち1個のみである:

- strict
- weighted

Queue Management Type/キュー管理タイプ - このインターフェイスでキューに使用されるキューの深さ管理技法。 これはデバイスがキュー毎に独立的設定をサポートする場合のみ使用される。
キュー管理タイプは次のうち1個のみである:

Taildrop

8.6 スタック・メニュー



このメニューにある機能はスタック可能イーサネット・コネクション・ブレードで提供される。

8.6.1 構成

8.6.1.1 ユニット・コンフィグ

Configuration

Unit Config | Archive Copy

Switch ID:	1
Serial Number:	SQ836MD00041
Role:	Mgmt Switch
Auto Upgrade:	Disable
MAC Address:	00:1E:68:C6:05:82
Hardware Management Preference:	Unassigned
Priority:	Unasssigned
Switch Type:	0xd5140002
Current Status:	Ready
Switch Description:	SB11 L2+ Switch Stacking System - 44 GE, 2 10GE
Detected Code Version:	0.16
Detected Code in Flash:	0.16
Up Time:	26103 seconds

* = mandatory

Apply　Refresh

図 ： スタック・ユニット・コンフィグ

選択基準

Switch ID/スイッチID - スタック・ユニットのリストを表示する。 選択されたユニットの詳細が表示される。 スタックの新たなメンバーを再構成できる、管理者のみに見えるCreateオプションもある。

Auto（オート） Upgrade/自動更新 - IBPに自動更新機能を有効化または無効化する。 IBPがスタックに参加することが必要でそのファームウェア・バージョンがスタック・マスターより低い場合、自動ファームウェア更新はこの機能がスタック・マスターで有効化されていれば実行される。

Priority/プライオリティ - 管理者がこのユニットを他のユニットに優先して管理ユニットにするかを示す欄である。 この設定のデフォルト値は1である。 優先レベルを0にすると、デバイスは管理ユニットになれない。 この欄は読みのみのユーザーには構成できない。

構成可能データ

Switch ID/スイッチID - スタック内で選択されたIBPのスイッチIDを表示する。 これは選択されたIBPのスイッチIDを再番号付けするために管理者により変更されえる。 この欄は読みのみのユーザーには構成できない。

構成不可能なデータ

Serial Number/連番 - 　このIBP.の一意なボックス連番を表示する。

Role/機能 - 選択されたIBPがマスターかスレーブかを表示する。

MAC Address/MACアドレス - IBPユニットのMACアドレス。

Hardware Management Preference/ハードウェア管理優先度 - このユニットが管理ユニットになれるかを示す2バイト欄。 この値が0に設定された場合、ユニットは管理ユニット機能をサポートできなくなる。 より値が高いユニットは他の値が低いユニットより管理機能を実行することを優先されることを意味する。 装置メーカーがこの欄は設定する。

Switch Type/スイッチ・タイプ - 選択されたユニットのハードウェア・タイプを識別する。 これは32ビットのデータ欄である。

Current Status/現在の状態 - 選択されたユニットの状態を表示する。 とりうる値:

- Ready
- Unsupported
- Code Mismatch
- Config Mismatch
- Not Present
- Code Updating

Switch Description/スイッチの内容 - 装置を識別するために使用される80バイトのデータ欄を表示する。

Detected Code Version/検出コード・バージョン - 検出されたコードのリリース番号とバージョン番号。

Detected Code in Flash/フラッシュメモリ内検出コード - フラッシュメモリに保存されているコードのリリース番号とバージョン番号を表示する。

Up Time/稼働時間 - IBPの直前再起動以降の相対時間を表示する。

コマンドボタン

Apply - IBP を画面の値で更新する。 IBPにパワー・サイクル後、設定を保持させるには、保存を実行しなければならない。. .。

Delete/削除 - スタックから選択されたユニットを削除する。

To be Master/マスターにする - 選択されたユニットをスタック・マスターにする。

Refresh/更新 - デフォルト値は3600である。

8.6.1.2　　アーカイブ･コピー



図 ： スタック･アーカイブ･コピー

選択基準

Unit/ユニット - 管理ユニット以外のスタックにあるすべてのユニットをリストする。

コマンドボタン

Apply - ユニット･セレクタにより指定されたスタック･ユニットに管理ユニットからコードをコピーする。

Download Archive/ダウンロード･アーカイブ - アーカイブ･ファイルをIBPにダウンロードする。

8.6.2 情報

8.6.2.1 サマリ

Information

Summary | Port Summary | Port Counters | Port Counters Detail

Switch ID	ID	Role	MAC Address	Priority	Current Status	Code Version
1	Encl-CB1	Mgmt Switch	00:1E:68:C6:05:82	Unassigned	Ready	0.16

Refresh

図 ： スタック･サマリ

構成不可能なデータ

Switch ID/スイッチID - ユニットのIDを表示する。 スタックに許可された最大ユニット数は8台である。

ID - ユニットの識別子を表示する。

Role/機能 - この欄はユニットがマスターかスレーブかを示す。

MAC Address/MACアドレス -IBPユニットのMACアドレス。

Priority/プライオリティ - 管理者がこのユニットを他のユニットに優先して管理ユニットにするかを示す2バイト欄である。 この設定のデフォルト値は1である。 優先レベルを0にすると、デバイスは管理ユニットになれない。 nt unit. この欄は読みのみのユーザーには構成できない。

Current Status/現在の状態 - この欄はユニットの状態を示す。 状態を示す5個の値がある：

– Ready
– Unsupported
– CodeMismatch
– ConfigMismatch
– NotPresent
– Code Updating

Code Version/コード･バージョン - この欄はユニットに検出されたコードのバージョンを示す。

コマンドボタン

Refresh/更新 - デフォルト値は3600である。

8.6.2.2　　ポート･サマリ

所与のスタックにあるすべてのスタック可能インターフェイスの統計を示す。

Information

Summary | Port Summary | Port Counters | Port Counters Detail

Unit	Interface	Configured Stack-mode	Running Stack-mode	Link Status	Link Speed (Gb/s)
1	Stack 1	N/A	Stack	Link Down	12
1	Stack 2	N/A	Stack	Link Down	12

Refresh

図 ： スタック･ポート･サマリ

構成不可能なデータ

Unit/ユニット - ユニットを表示する。.

Interface/インターフェイス - 所与のユニットにあるスタック可能インターフェイスを表示する。

Configured Stack Mode/構成スタック･モード - 所与のインターフェイスに構成されたモードを表示する。構成されたモードが、ポートが位置するユニットにある、NVRAMに直ちに保存されても、実行時モードは変更されない。

Running Stack Mode/実行スタック･モード - スタック可能インターフェイスの実行時モードを表示する。

Link Status/リンク･ステータス - ポートのリンク･ステータス(UP/DOWN)を表示する。

Link Speed (Gb/s)/リンク速度 - スタック･ポートの最高速度を表示する。

コマンドボタン

Refresh/更新 - ページ上のデータを更新する。

8.6.2.3　　ポート･カウンター

所与のスタックにあるすべてのスタック可能インターフェイスのカウンターを示す。

Information

Summary | Port Summary | Port Counters | Port Counters Detail

Unit	Interface	Transmit			Recieve		
		Data Rate (Mb/s)	Error Rate (Errors/s)	Total Errors	Data Rate (Mb/s)	Error Rate (Errors/s)	Total Errors
1	Stack 1	0	0	0	0	0	0
1	Stack 2	0	0	0	0	0	0

Refresh

図 ： スタック･ポート･カウンター

構成不可能なデータ

Unit/ユニット -　ユニットを表示する。.

Interface/インターフェイス - 所与のユニットにあるスタック可能インターフェイスを表示する。

送受信統計

- **Data Rate (Mb/s)/データ速度 - スタック･ポート上の速度概数を表示する。**
- **Error Rate (Errors/s)　-スタック･ポート上のエラー頻度概数を表示する。**
- **Total Errors/合計エラー数 - 起動以降のエラー合計値を表示する。 カウンターはラップできる。**

コマンドボタン

Refresh/更新 - ページ上のデータを更新する。

8.6.2.4　ポート･カウンターの詳細

Information

Summary | Port Summary | Port Counters | Port Counters Detail

Unit	Interface	Statistics
1	Stack 1	RBYT:0 RPKT:0 TBYT:0 TPKT:0 RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0 TAGE:0 TABRT:0
1	Stack 2	RBYT:0 RPKT:0 TBYT:0 TPKT:0 RFCS:0 RFRG:0 RJBR:0 RUND:0 ROVR:0 TAGE:0 TABRT:0

Refresh　Clear Counters

図 ： スタック･ポート･カウンターの詳細

所与のスタックにあるすべてのスタック可能インターフェイスの診断情報を示す。

構成不可能なデータ

Unit/ユニット - ユニットを表示する。.

Interface/インターフェイス - 所与のユニットにあるスタック可能インターフェイスを表示する。

Statistics/統計 - デバッグとステータス情報を含むドライバーにより埋められる3個のテキスト欄(80字の文字列)を表示する。

コマンドボタン

Refresh/更新 - ページ上のデータを更新する。

Clear Counters/カウンター･クリア - スタック･ポートの統計をリセットする。

9　　コマンド･レファレンス

コマンド･ライン･インタフェイス (CLI)構文、表記規則、用語をこの節で説明する。 各CLIコマンドを次に要約される構造により説明する。

9.1　　CLIコマンド･フォーマット

コマンドには値、パラメータ、またはこれら両方が続く。

例1

IP address <ipaddr> <netmask> [<gateway>]

- **IP address** はコマンド名である。
- **<ipaddr> <netmask>** はこのコマンドに必要な値である。
- **[<gateway>]** はこのコマンドのオプション値である。

例 2

snmp-server host <loc>

- **snmp-server host** はコマンド名である。
- **<loc>** はこのコマンドに必要なパラメータである。

例 3

clear vlan

- **clear vlan** はコマンド名である。

コマンド

太字の斜体でないフォントは表示されたとおりにタイプすること。

© 2010 富士通テクノロジー･ソリューションズ

9.2　CLIモード・ベースのトポロジー

パラメータ

パラメータは記述順に依存する。

斜体太字は名前または番号で置換する。 名前パラメータの一部として空白を使用するためには、次のように二重引用符で囲むこと： "System Name with Spaces".

パラメータは、必須の値、オプション値、選択詩、または組合わせでありうる。

- <parameter>. 山括弧＜＞は必須パラメータを括弧とその中の文字列に代えて入力しなければならないことを示す。
- [parameter]. 角括弧[ ]はオプション・パラメータを括弧とその中の文字列に代えて入力できることを示す。
- 選択 1｜ 選択 2. ｜は両側パラメータのうち 1 個のみ入力しなければならないことを示す。波括弧 { } はパラメータを 1 個、選択リストから選択しなければならないことを意味する。

値

ipaddr　このパララータは有効なIPアドレスであり、0から255までの範囲の4個の十進バイト数から構成される。すべてのIPパラメータのデフォルト値は零からなる (すなわち 0.0.0.0)。 インターフェイスIPアドレス0.0.0.0は無効である。

macaddr　MACアドレスのフォーマットはたとえば00:06:29:32:81:40のようにコロンで区画された6個の16進数である。

areaid　エリア IDはピリオドで区画された十進数で入力できる (たとえば 0.0.0.1)。 エリアID 0.0.0.0はバックボーンに予約されている。 エリアIDはIPアドレスと同じ形式であるが、IPアドレスとは別個のものである。 サブネット式ネットワークのIPネットワーク番号をエリアIDに使用できる。

routerid　T<router id>の値は4個の10進数字をピリオドで区画した表記とする。(たとえば、0.0.0.1) 0.0.0.0は無効なルーターIDである。

slot/port　このパラメータは有効なスロット番号、及び、有効なポート番号を示す。 たとえば、0/1はスロット番号0、ポート番号1を意味する。<slot/port>欄は標準のスラッシュ (/) で区切られた有効なスロットスロット番号と有効なポート番号からなる。

logical slot/port　このパラメータは割当てられた論理スロット番号、及び、論理ポート番号を示す。 ポートチャネル (LAG)の場合に該当する。 オペレータは論理スロット番号、及び、論理ポート番号を使用してポート・チャネルを構成できる。

表記規則

リモート・ホスト、ワークステーション、または、ネットワークへのリンクを定義するためにネットワーク・アドレスは使用される。 ネットワーク・アドレスは次の構文を用いて示される。

アドレス・タイプ	フォーマット	(範囲:
IPAddr	A.B.C.D	0.0.0.0 to 255.255.255.255
MacAddr	YY:YY:YY:YY:YY:YY	16進数ペア

表; ネットワーク・アドレスの構文

"System Name with Spaces"等の二重引用符はユーザー定義文字列を設定する。 名前のパラメータの一部として空白を使用するには、二重引用符で囲まなければならない。

しかし空白文字列 ("") はユーザー定義文字列として無効である。 コマンドの完成はコマンド語を一意に識別するために十分なコマンド文字がタイプされたときにコマンドのスペリングを完了する。 コマンドは<enter>をタイプ (コマンド略語) して実行される、または、コマンド語は<tab>または<space bar>をタイプして (コマンドの完成) 完了できる。

'Err'値は要求された値は内部ではアクセス不可であったことを意味する。 これは起きては成らないことであり、不正処理がソフトウェアにあることを示す。

'- - -'値は値が不明であることを示す。

注釈

CLIにより、テストまたは構成スクリプトを書くとき、および、より読みやすくするために、コマンド・プロンプトで1行注釈をタイプすることができる。 感嘆符('!')文字はコメントの開始をフラッグする。 コメント・フラッグ文字はコマンド行のどこでも単語を開始でき、この文字以降すべての入力内容は無視される。 '!'文字で始まるコマンド行はコメント行として認識されパーサーには無視される。

次にいくつか事例を示す:

```
! Script file for displaying the ip interface
! インターフェイスの情報を表示する
show ip interface 1/0/1 !最初のインターフェイスんついての情報を表示する
! 次のインターフェイスんついての情報を表示する
show ip interface 1/0/2
! スクリプト・ファイルの終了
```

9.3 システム情報と統計的コマンド

9.3.1 show arp

このコマンドはIBPと他のデバイスとの接続状態を表示する。 アドレス解決プロトコル (ARP) キャッシュはIBPと交信中のIPステーションのMACアドレスを識別する。

構文
show arp

初期設定

無

コマンド・モード

特権 EXEC

表示メッセージ

MAC Address/MACアドレス: IBPが転送またはフィルタリング情報を持つユニキャストMACアドレス。 フォーマットは、コロンで区画された6個の2桁16進数である。 たとえば: 00:23:45:67:89:AB

IP Address / IPアドレス: インターフェイス毎に割当てられたIPアドレス。

インターフェイス: 有効なスロット番号及び有効なポート番号。

9.3.2 show calendar

このコマンドはシステム・クロックを表示する。

Syntax
show calendar

初期設定

無

コマンド・モード

特権EXEC

表示メッセージ

現在時刻: システム時刻を表示する

© 2010 富士通テクノロジー・ソリューションズ

9.3.3 show eventlog

このコマンドはシステムからのエラー・メッセージを含むイベント・ログを表示する。 イベント・ログはシステム・リセット時に消去されない。

Syntax
show eventlog

初期設定

無

コマンド・モード

特権EXEC

表示メッセージ

File/ファイル： イベントが発生したファイル。

Line/行： イベントの行番号。

Task Id/タスクID: イベントのタスクID。

Code/コード： イベント・コード。

Time/時刻： 当該イベントの発生時刻。

(注記: イベント・ログ情報はIBPをリセットしても保持される。

9.3.4 show running-config

このコマンドはIBPでサポートされる現在の異なるプロトコル・パッケージの設定を表示、取得するために使用される。 このコマンドはデフォルト値とは異なる値を持つ設定や構成によるコマンドのみ表示、取得する。 その出力はスクリプト・フォーマットで表示され、これは同じ構成で他のIBPを構成するために使用できる。

スクリプト名がある場合、その出力は構成すクリップとにリダイレクトされる。 [all]オプションはデフォルト値と同じ値を含む設定や構成によるすべてのコマンドの表示、取得も可能にする。 <scriptname>オプションがファイル拡張子".scr"とともに与えられた場合、出力はスクリプト・ファイルにリダイレクトされる。

Syntax
show running-config [all] [<scriptname>] [|]

[all] - デフォルト値と同じ値を含む設定や構成によるすべてのコマンドの表示、取得が可能になる。

[<scriptname>] - 出力を<scriptname>ファイルにリダイレクトする。

[|] - 出力変更子。

初期設定

なし

© 2010 富士通テクノロジー・ソリューションズ

コマンド・モード

特権EXEC

表示メッセージ

9.3.5 show sysinfo

このコマンドはIBP要約情報とサポートされるMIBを表示する。

Syntax
show sysinfo

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

System Description /システム内容：このIBPを識別するために使用される文字列。

System Name / システム名：このIBPを識別するために使用される名前。

System Location / システムの位置：このIBPの所在地を識別するために使用される文字列。 最大31文字までの英数字を使用できる。 工場側デフォルト値は空白である。

System Contact /システム責任者：このIBPの管理担当者を識別するために使用される文字列。 最大31文字までの英数字を使用できる。 工場側デフォルト値は空白である。

System Object ID/システム・オブジェクトID： 製造番号。

System Up Time/システム稼働時間：直前のIBP再起動以降経過した時間を日数、時間、分で表記

Current SNTP Synchronized Time/現在のSNTP同期化時間： 時間がSNTPサーバと同期化された時間。

MIBs Supported/サポートされるMIB： このエージェントによりサポートされるMIBのリスト。

9.3.6 show system

このコマンドはIBPシステム情報を表示する。

Syntax
show system

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

System Description /システム内容 -: このIBPを識別するために使用される文字列。

System Object ID/システム・オブジェクトID: 製造番号

システム情報

System Up Time/システム稼働時間: 直前のIBP再起動以降経過した時間を日数、時間、分で表記

System Name/システム名 : このIBPを識別するために使用される名前。

System Location/システム所在地 :このIBPの所在地を識別するために使用される文字列。 最大31文字までの英数字を使用できる。 工場側デフォルト値は空白である。

System Contact/システム責任者 : このIBPの管理担当者を識別するために使用される文字列。最大31文字までの英数字を使用できる。 . 工場側デフォルト値は空白である。

MAC Address/MACアドレス:インバンド接続のために使用されるMACアドレス。

Web Server/ウェブ・サーバ: ウェブ・サーバ機能を有効化/無効化するために表示される。

Web Server Port/ウェブ・サーバ・ポート: ウェブ・サーバのhttpポートを表示する

Web Server Java Mode/ウェブ・サーバJAVAモード: IBPがヘッダー・フレームにあるJavaアプレットにアクセスを許可するかを指定する。 有効化されているとアプレットを見ることができる。 工場側デフォルトは無効化されている。

Protocol Current/現在プロトコル: 現在使用中のネットワーク・プロトコルを示す。 オプションはbootp | dhcp | noneである。

DHCP Client Identifier TEXT/DHCPクライアント識別子TEXT: このIBPのためのDCHPクライアント識別子

9.3.7 show hardware

このコマンドはIBPnインベントリ情報を表示する。

Syntax
show hardware

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

System Description /システム内容:このIBPの製品名を識別するために使用される文字列。

Machine Type/マシンタイプ: 重要製品データにより定義されたマシン・モデルを指定する。

Machine Model/機種: 重要製品データにより定義されたマシン・モデルを指定する。

Serial Number/連番: このIBPに一意のシリアル番号。

Label Revision Number/ラベル改訂番号: このIBPのラベル改訂連番は製造のために使用される。

パーツ番号: パーツ製造番号。

Hardware Version/ハードウェア・バージョン: このIBP.のハードウェア・バージョン。最初のバイトはメジャー・バージョンを指し、2番目のバイトはマイナー・バージョンを指す。

Loader Version/ローダー・バージョン - 現在IBPで実行中のローダー・コードのリリース・バージョン・メンテナンス番号 たとえば。たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。

Boot Rom Version/起動ROMバージョン - 現在IBPで実行中の起動ROMコードのリリース・バージョン・メンテナンス番号 たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。

Operating Code Version/ 動作コード・バージョン: 現在IBPで実行中のコードのリリース・バージョン・メンテナンス番号 たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。e '1.2'.

(注記: 下記の情報はSFP/SFP+モジュールをプラグインすると表示される。

Module 1 /モジュール1 : 検出さたモジュール・タイプ、たとえば、SFPまたはSFP+

Status/ステータス: この検出されたモジュールの状態、たとえばOKまたはNot Supported。

ギガビット・イーサネット準拠コード:SFP/SFP+トランシーバのベンダー名は、会社の正式名、会社名の一般に通用している略称。

Vendor Name/ベンダー名: メーカー名。

Vendor Part Number/ベンダー・パーツ番号: SFP+トランシーバのベンダーが割当てたパーツ番号。

Vendor Serial Number/ベンダー連番: ベンダーが割当てた連番。

Vendor Revision Number/ベンダー改訂番号: ベンダーが割当てたパーツ番号の改訂レベル。

Vendor Manufacturing Date/ベンダー製造日: ベンダーの製造日。

Additional Packages/追加パッケージ: このシステムに一体化された追加パッケージを表示する。

9.3.8 show version

このコマンドはIBPのバージョン情報を表示する。

Syntax
show version

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Serial Number/連番: このIBPに一意のボックス連番。

Hardware Version/ハードウェア・バージョン: このIBP.のハードウェア・バージョン。 これは4部分に分割される。 最初のバイトはメジャー・バージョンを指し、2番目のバイトはマイナー・バージョンを指す。

Number of ports/ポート数 : IBPにある物理ポートの個数を示す。

Label Revision Number/ラベル改訂番号: このIBPのラベル改訂連番は製造のためにされる。

パーツ番号: パーツ製造番号。

Machine Model/機種: 機種のうちの型式。

Loader Version/ローダー・バージョン : 現在IBPで実行中のローダー・コードのリリース・バージョン・メンテナンス番号 たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。

Operating Code Version/ 動作コード・バージョン : 現在IBPで実行中のコードのリリース・バージョン・メンテナンス番号 たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。

Boot Rom Version/起動ROMバージョン : L現在IBPで実行中の起動ROMコードのリリース・バージョン・メンテナンス番号 たとえば、リリースが1でバージョンが2の場合、フォーマットは'1.2'になる。

9.3.9 show tech-support

このコマンドはトラブルシューティングに必要なIBP情報を表示する。

Syntax
show tech-support

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

9.3.10 show loginsession

このコマンドはIBPへの現在のTelnetとシリアルポート接続を表示する。

Syntax
show loginsession

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

ID: ログイン・セッションID

User Name/ユーザー名: シリアルポートまたはTelentによりログインのためにユーザーが使用する名前。空白エントリに名前を入力してIBPに新たなユーザーを追加できる。 ユーザー名は最大8文字、大文字・小文字を区別しない。 adminとguest2人のユーザーが工場側デフォルト値として含まれている。

Connection From/接続元: Telnetクライアント・マシンまたはシリアルポート接続のEIA-232のIPアドレス。

アイドル時間: このセッションがアイドルである時間。

Session Time/セッション時間: このセッションの接続されている合計時間。

Session Type/セッション・タイプ: セッション・タイプを示す: telnet、シリアル、または、SSH。

9.4 デバイス構成コマンド

9.4.1 インターフェイス

9.4.1.1 show interface status

このコマンドはシステムのポート監視情報を表示する。

Syntax
show interface status {<slot/port> | all}

<slot/port> - 必要なインターフェイス番号である。

all - このパラメータはすべてのインターフェイスについて情報を表示する。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Intf: 物理スロットと物理ポート。

Type/種類:空白でない場合、この欄は当該ポートが特別な種類のポートであることを示す。 とりうる値:

Source/ソース - ポートは監視ポートである。

PC Mbr - このポートはポートチャネルのメンバーである(LAG)。

Dest/ターゲット - このポートはプローブ・ポートである。

管理モードポート制御管理ステートを選択する。 ポートはネットワークに許可されるには有効化されていなければならない。 – ポートは有効化または無効化できる。 デフォルト設定は有効化されている。 .

E-Keying Status/E-KEY機能の状態: キー機能の状態を示す。

Physical Mode/物理モード: 必要なポート速度と二重モードを選択する。 自動ネゴシエーションのサポートを選択すると、二重モードと速度が自動ネゴシエーションにより設定される。 ポートの最高性能 (全二重で100Mbps)が通知されることに注意する。 さもなければ、このオブジェクトはポートの二重モードと転送速度を決める。 工場側デフォルトはAuto (オート) である。

Physical Status/物理ステータス: ポート速度と二重モードを示す。

リンク・ステータス リンクがアップかダウンかを示す。

Link Trap/リンク・トラップ:このオブジェクトはリンク・ステータスが変化したときトラップを送るかを定義する。デフォルト設定は有効化されている。

Flow Mode/フロー・モード: フロー制御モードを表示する。

Capabilities Status/機能ステータス: インターフェイスの機能を表示する。

© 2010 富士通テクノロジー・ソリューションズ

9.4.1.2 show interface counters

このコマンドは特定のインターフェイスまたはすべてのインターフェイスの統計サマリを表示する。

Syntax
show interface counters {<slot/port> | all}

<slot/port> - 必要なインターフェイス番号である。

all - このコマンドはすべてのインターフェイスについて統計情報を表示する。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

引数が'<slot/port>'のときの表示パラメータ:

Packets Received Without Error/エラー無しで受信されたパケット:プロセッサに受信されたパケット総数(ブロードキャスト・パケットとマルチキャスト・パケットを含む)

Packets Received With Error/エラー有りで受信されたパケット: エラーのため受信できなかったパケット数

Broadcast Packets Received/受信されたブロードキャスト・パケット:ブロードキャスト・アドレスにダイレクトされた受信パケット総数 これにはマルチキャスト・パケットが含まれないことに注意する。

Packets Transmitted Without Error/エラー無しで送信されたパケット:インターフェイスから送信されたパケットの総数。

Transmit Packets Errors/送信パケット・エラー数: エラーのため送信できなかったパケット数。

Collisions Frames/コリジョン・フレーム数: 当該イーサネット・セグメントでのコリジョン総数。

Time Since Counters Last Cleared/直前のカウンター・クリア以降の時間:このポートの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒で示したもの。

引数が'all'のときの表示パラメータ:

Interface/インターフェイス: 物理スロットと物理ポート、または、論理スロットと論理ポート。

Summary/要約: すべてのポートの統計の合算。

Packets Received Without Error/エラー無しで受信されたパケット:受信されたパケット総数(ブロードキャスト・パケットとマルチキャスト・パケットを含む)。

Packets Received With Error/エラー有りで受信されたパケット: エラーのため受信できなかったパケット数

Broadcast Packets Received/受信されたブロードキャスト・パケット:ブロードキャスト・アドレスにダイレクトされた受信パケット総数 これにはマルチキャスト・パケットが含まれないことに注意する。

Packets Transmitted Without Error/エラー無しで送信されたパケット: 送信されたパケット総数。

Transmit Packets Errors/送信パケット・エラー数: エラーのため送信できなかったパケット数。

© 2010 富士通テクノロジー・ソリューションズ

Collisions Frames/コリジョン・フレーム数: 当該イーサネット・セグメントでのコリジョン総数。

このコマンドは引数に基づいて特定のポートまたはすべてのCPUトラフィックの詳細統計を表示する。

Syntax
show interface counters detailed {<slot/port> | switchport}

<slot/port> -必要なインターフェイス番号である。

switchport - このパラメータはIBP全体またはすべてのインターフェイスを指定する。

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

引数が'<slot/port>'のときの表示パラメータ:

Total Packets Received (Octets)/受信パケット合計数 (オクテット) :ネットワークで受信された(失敗したパケットにあるものを含む)データ・オクテット総数 (フレーム・ビットを除きFCSオクテットを含む). このオブジェクトはイーサネット使用度の適度な推計値として使用できる。 より高精度が必要な場合、etherStatsPktsとetherStatsOctetsオブジェクトが共通間隔の前後にサンプルされる必要がある。 この方程式の結果は0から100パーセントまでの尺度によるイーサネット・セグメントの使用率パーセントである使用率の値である。

Packets Received 64 Octets/64オクテット受信パケット: 長さ64オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 65-127 Octets / 65-127オクテットの受信パケット: 長さ65と127オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 128-255 Octets /128-255オクテットの受信パケット: 長さ128と255オクテットの受信された (フレーム・ビットを除きFCSオクテットを含む).パケット総数 (失敗したパケットを含む) 。

Packets Received 256-511 Octets / 256-511オクテットの受信パケット: 長さ256と511オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received 512-1023 Octets / 512-1023オクテットの受信パケット: 長さ512と1023オクテットの受信された (フレーム・ビットを除きFCSオクテットを含む).パケット総数 (失敗したパケットを含む)。

Packets Received 1024-1518 Octets / 1024-1518オクテットの受信パケット -

長さ1024と1518オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Received >1522 Octets/1522オクテットを超える受信パケット: 長さ1522オクテット超の受信され(フレーム・ビットを除きFCSオクテットを含む)、良好に形成されたパケット総数。

Packets RX and TX 64 Octets/64オクテット送受信パケット:
長さ64オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets RX and TX 65-127 Octets /65~127オクテットの送受信パケット -長さ65と127オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 128-255 Octets /28-255オクテットの送受信パケット: 長さ128と255オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)　。

Packets RX and TX 256-511 Octets/ 256-511オクテットの送受信パケット -　: 長さ256と511オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)　。

Packets RX and TX 512-1023 Octets 512-1023オクテットの送受信パケット -　: 長さ512と1023オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)　。

Packets RX and TX 1024-1518 Octets / 1024-1518 オクテットの送受信パケット -: 長さ1024と1518オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)　。

Packets RX and TX 1519-2047 Octets / 1519-2047 オクテットの送受信パケット:

長さ1519と1522オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 2048-4095 Octets 2048-4095オクテットの送受信パケット :

長さ2048と4095オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets RX and TX 4096-9216 Octets 4096-9216 オクテットの送受信パケット:

長さ4096と9216オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Total Packets Received Without Error/エラー無しで受信されたパケット総数

Unicast Packets Received/受信されたユニキャスト・パケット: 高レベル・レイヤー・プロトコルにデリバリされたユニキャスト・パケット数。

Multicast Packets Received/受信されたマルチキャスト・パケット:マルチキャスト・アドレスにダイレクトされた受信された良好なパケットの総数。 この総数にはブロードキャスト・アドレスにダイレクトされたパケットは含まれないことに注意する。

Broadcast Packets Received/受信されたブロードキャスト・パケット:ブロードキャスト・アドレスにダイレクトされた受信された良好パケットの総数。 これにはマルチキャスト・パケットが含まれないことに注意する。

Total Packets Received with MAC Errors/MACエラー有りで受信されたパケット総数

受信ジャバー：長さ1518オクテット超の受信され(フレーム・ビットを除きFCSオクテットを含む).、良好に形成され、さらに整数のオクテット数による失敗したフレーム・チェック・シーケンス(FCSエラー)または非整数のオクテット数による失敗したFCS(アラインメント・エラー)があるパケット総数。 このジャバー定義はIEEE-802.3 セクション8.2.1.5 (10BASE5) とセクション10.3.1.4 (10BASE2)の定義とは異なる。 この文書ではジャバーをパケットが20msを超える条件として定義する。ジャバー検出許容範囲は20msから150msである。

Undersize Received/受信されたサイズ不足パケット:長さ64オクテット未満の受信され(フレーム・ビットを除きFCSオクテットを含む)、良好なCRCによるパケット総数。

Fragments Received/受信されたフラグメント:長さ64オクテット未満の受信され(フレーム・ビットを除きFCSオクテットを含む)、エラーCRCがあるパケット総数。

Alignment Errors/アラインメント・エラー: 64ビット以上1518以下の長さ(フレーム・ビットを除きFCSオクテットを含む) であるがオクテット数が整数ではない不正FCSがある受信されたパケット総数。

FCS Errors/FCSエラー: 64ビット以上1518以下の長さ(フレーム・ビットを除きFCSオクテットを含む) であるがオクテット数が整数の不正FCSがある受信されたパケット総数。

Overruns/オーバーラン:このポートが受信パケットにより過負荷状態となり、流入パケットに対応できなくなったために破棄されたフレーム総数。

MTU Errors/MTUエラー:このポートが流入パケットによりMTUより大きかったため破棄されたフレーム総数。

Total Packets Received with MAC Errors/MACエラー有りで受信されたパケット総数

Total Packets Transmitted (Octets)/送信パケット総数 (オクテット) :

Packets Transmitted 64 Octets/64オクテット送信パケット: 長さ64オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Transmitted 65-127 Octets/65～127オクテット送信パケット: 長さ65と127オクテットの受信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む)。

Packets Transmitted 128-255 Octets /送信された128-255オクテット・パケット: 長さ128と255オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 256-511 Octets /送信された256-511オクテット・パケット: 長さ256と511オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 512-1023 Octets / 送信された512-1023 オクテット・パケット: 長さ512と1023オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Packets Transmitted 1024-1518 Octets /送信された1024-1518オクテット・パケット-長さ1024と1518オクテットの受信または送信された(フレーム・ビットを除きFCSオクテットを含む).パケット総数(失敗したパケットを含む) 。

Max Frame Size/最大フレーム・サイズ: 最大フレーム・サイズを表示する。

Total Packets Transmitted Successfully/送信完了パケット総数

Unicast Packets Transmitted/送信されたユニキャスト・パケット:高レイヤー・プロトコルがユニキャスト・アドレスへの送信を要求したパケット総数で破棄されたものも送られなかったものも含む。

Multicast Packets Transmitted/送信されたマルチキャスト・パケット:高レイヤー・プロトコルがマルチキャスト・アドレスへの送信を要求したパケット総数で破棄されたものも送られなかったものも含む。

Broadcast Packets Transmitted/送信されたブロードキャスト・パケット: 高レイヤー・プロトコルにブロードキャスト・アドレスへの送信を要求されたパケット総数で破棄されたものも送られなかったものも含む。

Tx Oversized/超過Tx:最大許容フレーム・サイズを超過したフレーム総数。 このカウンターは1秒当たり10メガビット出1秒当たり815カウントが最大インクリメントされる。

Total Transmit Errors/送信エラー総数

FCS Errors/FCSエラー: 64ビット以上1518以下の長さ(フレーム・ビットを除きFCSオクテットを含む) であるがオクテット数が整数の不正FCSがある送信されたパケット総数。

Underrun Errors/アンダーラン・エラー: 送信FIFOバッファーがフレーム送信中に空になったため破棄されたフレーム総数

Total Transmitted Packets Discards/送信パケット破棄総数

Single Collision Frames/シングル・コリジョン・フレーム数:送信がちょうどコリジョン1回で妨害された特定インターフェイス上で送信が完了したフレーム数。

Multiple Collision Frames/複数コリジョン・フレーム数:送信が1回を超えるコリジョンで妨害された特定インターフェイス上で送信が完了したフレーム数。

Excessive Collisions/過度コリジョン:過度のコリジョンにより特定インターフェイスでの送信障害を起こしたフレーム数。

Time Since Counters Last Cleared/直前のカウンター・クリア以降の時間:このポートの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒で示したもの。

引数が'switchport'のときの表示パラメータ:

Total Packets Received (Octets)/受信パケット総数 (オクテット): プロセッサにより受信されたデータ・オクテット総数 (フレーム・ビットを除きFCSオクテットを含む)。

Packets Received Without Error/エラー無しで受信されたパケット: プロセッサに受信されたパケット総数 (ブロードキャスト・パケットとマルチキャスト・パケットを含む) 。

Unicast Packets Received/受信されたユニキャスト・パケット: 高レベル・レイヤー・プロトコルにデリバリされたユニキャスト・パケット数。

Multicast Packets Received/受信されたマルチキャスト・パケット: マルチキャスト・アドレスにダイレクトされた受信されたパケットの総数。 この総数にはブロードキャスト・アドレスにダイレクトされたパケットは含まれないことに注意する。

Broadcast Packets Received/受信されたブロードキャスト・パケット: ブロードキャスト・アドレスにダイレクトされた受信パケット総数。 これにはマルチキャスト・パケットが含まれないことに注意する。

Receive Packets Received/破棄された受信パケット: 高レイヤー・プロトコルへのデリバリを妨げるエラーが検出されなくても廃棄されたインバウンド・パケット数。 パケット廃棄の考えうる理由はバッファー容量を空けるため。

Octets Transmitted/送信されたオクテット - インターフェイスから送信された、フレーム文字を含むオクテット総数

Packets Transmitted Without Errors/エラー無しで送信されたパケット - インターフェイスから送信されたパケット総数

Unicast Packets Transmitted/ 送信されたユニキャスト・パケット - 高レイヤー・プロトコルにサブネットワーク・ユニキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む

Multicast Packets Transmitted/ 送信されたマルチキャスト・パケット - 高レイヤー・プロトコルにマルチキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む

Broadcast Packets Transmitted/ 送信されたブロードキャスト・パケット - 高レイヤー・プロトコルにブロードキャスト・アドレスへの送信を要求されたパケット総数で落とされたものも送られなかったものも含む。

© 2010 富士通テクノロジー・ソリューションズ

Transmit Packets Discarded/廃棄された送信パケット - 高レイヤー・プロトコルへのデリバリを妨げるエラーが検出されなくても廃棄されたアウトバウンド・パケット数。 パケット廃棄の考えうる理由はバッファー容量を空けるためなど。

Most Address Entries Ever Used/使用された最大アドレス・エントリ - 直前の再起動以降IBPが学習した転送データベース・アドレス・テーブルのエントリの最大数

Address Entries Currently in Use/現在使用中のアドレス・エントリ: このIBPの転送データベース・アドレス・テーブルにある学習エントリと静的エントリの数。

Maximum VLAN Entries/最大VLANエントリ - IBPで許可された仮想LAN (VLANs) の最大数

Most VLAN Entries Ever Used/使用された最大VLANエントリ - 直前再起動以降このIBPでアクティブなVLANの最大数

Static VLAN Entries/静的VLANエントリ - このIBPにある静的に生成された現在アクティブなVLANエントリ数

Dynamic VLAN Entries/動的VLANエントリ: GVRP登録によりに生成されたこのIBPで現在アクティブなVLANエントリ数。

VLAN Deletes/削除されたVLAN - 直前再起動以降生成され、削除されたこのIBPにあるVLANの数

Time Since Counters Last Cleared/カウンターの直前クリア以降の経過時間 - このIBPの統計が最後にクリアされて以降経過した時間を日数、時間、分、秒までで示したもの

9.4.1.3 show interface IBP

このコマンドはすべてのCPUトラフィックの統計サマリを表示する。

Syntax
show interface IBP

初期設定

なし

コマンド・モード

特権EXEC

表示メッセージ

Packets Received Without Errors/エラー無しで受信されたパケット - プロセッサに受信されたパケット総数 (ブロードキャスト・パケットとマルチキャスト・パケットを含む)

Broadcast Packets Received/受信されたブロードキャスト・パケット: ブロードキャスト・アドレスにダイレクトされた受信パケット総数 これにはマルチキャスト・パケットが含まれないことに注意する。

Packets Received With Error/エラー有りで受信されたパケット: エラーが有るため高レイヤー・プロトコルにデリバリされえなかったインバウンド・パケット数

Packets Transmitted Without Error/エラー無しで送信されたパケット: インターフェイスから送信されたパケットの総数。

Broadcast Packets Transmitted/送信されたブロードキャスト・パケット: 高レイヤー・プロトコルがブロードキャスト・アドレスへの送信を要求したパケット総数で破棄されたものも送られなかったものも含む。

Transmit Packets Errors/送信パケット･エラー数: エラーのため送信できなかったアウトバウンド･パケット数。

Address Entries Currently in Use/現在使用中のアドレス･エントリ: 学習されたエントリと静的エントリを含み、IBPで現在アクティブな転送データベース･アドレス･テーブルのエントリ総数。

Time Since Counters Last Cleared/直前のカウンター･クリア以降の時間: このIBPの統計の直前クリア以降経過した時間を日数、時間、分、秒で示したもの。

9.4.1.4 interface

このコマンドはインターフェイス構成モードに入るために使用される。

Syntax
interface <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

© 2010 富士通テクノロジー･ソリューションズ

9.4.1.5 インターフェイスの範囲

このコマンドによりインターフェイスレンジの設定モードに入ります。

Syntax
interface range {<slot/port> [- <slot/port>]} [, {<slot/port> [- <slot/port>]} [, {<slot/port> [- <slot/port>]} [, {<slot/port> [- <slot/port>]} [, {<slot/port> [- <slot/port>]}]]]]

<slot/port> -必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.1.6 速度・二重

このコマンドによりインターフェイスにspeedとduplexのモードを設定します。

Syntax
speed-duplex {10 | 100} {full-duplex | half-duplex}

100 - 100BASE-T

10 - 10BASE-T

full-duplex -全二重

half-duplex -半二重

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりインターフェイスにspeedとduplexのモードを設定します。

Syntax
speed-duplex all {10 | 100} {full-duplex | half-duplex}

100 - 100BASE-T

10 - 10BASE-T

full - duplex - 全二重

half - duplex - 半二重

all - このコマンドはすべてのインターフェイスを表します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.1.7 negotiate

このコマンドによりポートの自動ネゴシエーションを有効化します。デフォルト値は有効化です。

Syntax
negotiate no negotiate

no – このコマンドによりポートの自動ネゴシエーションを無効化します。

初期設定

有効化

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべてのインターフェイスの自動ネゴシエーションを有効化します。デフォルト値は有効化です。

Syntax
negotiate all no negotiate all

all - このコマンドはすべてのインターフェイスを表します。

no - このコマンドによりすべてのインタフェイスの自動ネゴシエーションを無効化します。

初期設定

有効化

コマンド・モード

グローバル・コンフィグ

9.4.1.8 capabilities

このコマンドによりインターフェイスレンジの特定の設定機能を設定します。

Syntax
capabilities {{10 | 100 } {full-duplex | half-duplex}} | {1000 full-duplex } no capabilities {{10 | 100 } {full-duplex | half-duplex}} | {1000 full-duplex }

10 - 10BASE-T

100 - 100BASE-T

1000 - 1000BASE-T

full-duplex - 全二重

half-duplex - 半二重

no - このコマンドによりポートの自動ネゴシエーションを無効化します。

初期設定

10 半二重、10 全二重、100 半二重、100 全二重、1000 全二重

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべてのインターフェイスレンジの機能を設定します。

Syntax
capabilities all {{10 | 100} {full-duplex | half-duplex}} | {1000 full-duplex } no capabilities all {{10 | 100} {full-duplex | half-duplex}} | {1000 full-duplex }

10 - 10BASE-T

100 - 100BASE-T

1000 - 1000BASE-T

full-duplex - 全二重

half-duplex - 半二重

all - このコマンドはすべてのインターフェイスを表します。

no - このコマンドによりポートの自動ネゴシエーションを無効化します。

初期設定

10 半二重、10 全二重、100 半二重、100 全二重、1000 全二重

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.4.1.9 storm-control flowcontrol

このコマンドによりIBPの802.3xフロー制御を有効化します。

注記：このコマンドは全二重モードのポートのみに適用されます。

Syntax
storm-control flowcontrol no storm-control flowcontrol

no – このコマンドによりIBPの802.3xフロー制御を無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

このコマンドにより特定のインターフェイスの802.3xフロー制御を有効化します。

注記：このコマンドは全二重モードのポートのみに適用されます。

Syntax
storm-control flowcontrol no storm-control flowcontrol

no – このコマンドにより特定のインターフェイスの802.3xフロー制御を無効化します。

初期設定

無効

コマンド・モード

インターフェイス・コンフィグ

9.4.1.10 shutdown

このコマンドによりポートを無効化します。

Syntax
shutdown no shutdown

no – このコマンドによりポートを有効化します。

初期設定

有効

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべてのインターフェイスレンジの機能を設定します。

Syntax
shutdown all no shutdown all

all - このコマンドはすべてのインターフェイスを表します。

no – このコマンドによりすべてのポートを有効化します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.4.1.11 MDI/MDIX

このコマンドにより物理ポートのMDI/MDIXモードを設定します。

Syntax
mdi {Auto (オート) | across | normal} no mdi

Auto (オート) - MDI 強制自動モード

across - MDIアクロスモード

normal - MDIノーマルモード

no – このコマンドによりmdiをデフォルト設定に戻します。

初期設定

ノーマル

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.4.2 L2 MACアドレスとマルチキャスト転送データベーステーブル

9.4.2.1 show mac-addr-table

このコマンドにより転送データベースエントリを表示します。パラメータをつけずにコマンドを入力するとテーブル全体が表示されます。任意のallパラメータを入力した場合も同様です。管理者がMACアドレスを入力して要求MACアドレスのテーブルエントリおよび要求MACアドレスのすべてのエントリを表示することもできます。

Syntax
show mac-addr-table [{<macaddr> < vlanid >|all}]

<macaddr> - MACアドレスを入力して要求MACアドレスのテーブルエントリを表示します。

<vlanid> - VLAN ID (範囲：1～4094)

all – このコマンドによりテーブル全体を表示します。

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

MAC Address/MACアドレス: IBPが転送またはフィルタリング情報を持つユニキャストMACアドレス。01:23:45:67:89:ABのように6個または8個の2桁の16進数がコロンで区切られて表示されます。IVLシステムの場合、MACアドレスは8バイトで表示されます。SVLの場合MACアドレスは6バイトで表示されます。**注記：このソフトウェアバージョンはIVLシステムのみに対応しています。**

インターフェイス： L2 MACアドレスが学習されたポート

if Index: このポートに関連するインタフェイステーブルエントリのインターフェイス番号を示します。

ステータス： エントリのステータス。

値の内容は以下のとおりです。

Static – 静的MACフィルタが定義された際、システムまたはユーザーにより追加された該当インスタンスの値

Learned - 受信トラフィックのソースMACアドレスを確認し、学習した該当インスタンスの値

Management - 該当インスタンスの値 (システムMACアドレス) は、dot1dStaticAddress の既存インスタンスの値となります。この値はインタフェイス3/1と判断され、VLANを有効化しルーティングを行うために使用されます。

Self - IBPの物理インタフェイスのアドレス (システムのMACアドレス) である、該当インスタンスの値

GMRP Learned - 該当インスタンスの値をGMRP経由で学習し、マルチキャストに適用します。

Other - どのカテゴリにも分類されない該当インスタンスの値

9.4.2.2 show mac-addr-table count

このコマンドにより転送データベースエントリの合計数、静的MACアドレス数および取得MACアドレス数、IBPで使用可能な最大アドレスを表示します。

Syntax
show mac-addr-table count

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Dynamic Address count: L2 MACアドレステーブルの取得MACアドレスの合計数

Static Address (User-defined) count: L2 MACアドレステーブルのユーザー定義アドレスの合計数

Total MAC Addresses in use: L2 MACアドレステーブルのアドレスの合計数

Total MAC Addresses available: L2 MACアドレステーブルでIBPが対応している最大値

9.4.2.3 show mac-addr-table interface

このコマンドにより転送データベースエントリを表示します。インタフェイス番号<slot/port>を使用し、FDBテーブルを検索できます。

Syntax
show mac-addr-table interface <slot/port>

<slot/port> - インタフェイス番号

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Mac Address: IBPが転送またはフィルタリング情報を持つユニキャストMACアドレス。01:23:45:67:89:ABのように6個または8個の2桁の16進数がコロンで区切られて表示されます。 IVLシステムの場合、MACアドレスは8バイトで表示されます。 SVLの場合MACアドレスは6バイトで表示されます。

VLAN ID: MACアドレスのVLAN ID

ステータス： エントリのステータス。

値の内容は以下のとおりです。

Static - 静的MACフィルタが定義された際、システムまたはユーザーにより追加された該当インスタンスの値

Learned - 受信トラフィックのソースMACアドレスを確認し、学習した該当インスタンスの値

Management - 該当インスタンスの値 (システムMACアドレス) は、 dot1dStaticAddress の既存インスタンスの値となります。この値はインタフェイス3/1と判断され、VLANを有効化しルーティングを行うために使用されます。

Self - IBPの物理インタフェイスのアドレス (システムのMACアドレス) である、該当インスタンスの値

GMRP Learned - 該当インスタンスの値をGMRP経由で学習し、マルチキャストに適用します。

Other - どのカテゴリにも分類されない該当インスタンスの値

9.4.2.4 show mac-addr-table vlan

このコマンドにより転送データベースエントリを表示します。VLAN IDによりFDBテーブルを検索できます。

Syntax
show mac-addr-table vlan <vlanid>

<vlanid> - VLAN ID (範囲： 1 – 4094)

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Mac Address: IBPが転送またはフィルタリング情報を持つユニキャストMACアドレス。01:23:45:67:89:ABのように6個または8個の2桁の16進数がコロンで区切られて表示されます。 IVLシステムの場合、MACアドレスは8バイトで表示されます。 SVLの場合MACアドレスは6バイトで表示されます。

インターフェイス： L2 MACアドレスが学習されたポート

ステータス： エントリのステータス。

値の内容は以下のとおりです。

Static - 静的MACフィルタが定義された際、システムまたはユーザーにより追加された該当インスタンスの値

Learned - 受信トラフィックのソースMACアドレスを確認し、学習した該当インスタンスの値

Management - 該当インスタンスの値 (システムMACアドレス) は、 dot1dStaticAddress の既存インスタンスの値となります。この値はインタフェイス3/1と判断され、VLANを有効化しルーティングを行うために使用されます。

Self - IBPの物理インタフェイスのアドレス (システムのMACアドレス) である、該当インスタンスの値

Other - どのカテゴリにも分類されない該当インスタンスの値

9.4.2.5 show mac-addr-table agetime

このコマンドにより転送データベースのアドレスエイジングタイムアウトを表示します。

Syntax
show mac-addr-table agetime

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Address Aging Timeout: 転送データベーステーブルの合計秒数を示します。

9.4.2.6 mac-addr-table aging-time

このコマンドにより転送データベースのアドレスエイジングタイムアウトを秒単位で設定します。

Syntax
mac-addr-table aging-time <10-1000000> no mac-addr-table aging-time

<10-1000000> - エイジングタイム、秒単位（範囲：10～1000000）

no - 転送データベースのアドレスエイジングタイムアウトを300秒に設定します。

初期設定

300

コマンド・モード

グローバル・コンフィグ

9.4.2.7 show mac-address-table multicast

このコマンドによりMFDB情報を表示します。 パラメータをつけずにコマンドを入力するとテーブル全体が表示されます。 *all*パラメータを入力した場合も同様です。任意のパラメータでMACアドレスを指定して、1つのMACアドレスのテーブルエントリを表示できます。

Syntax
show mac-address-table multicast {<macaddr> <vlanid> | all }

<macaddr> - MACアドレスを入力して要求MACアドレスのテーブルエントリを表示します。

<vlanid> - VLAN ID (範囲：1～4094)

all – このコマンドによりテーブル全体を表示します。

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Mac Address: IBPが転送またはフィルタリング情報を持つユニキャストMACアドレス。01:23:45:67:89:ABのように6個または8個の2桁の16進数がコロンで区切られて表示されます。 IVLシステムの場合、MACアドレスは8バイトで表示されます。 SVLの場合MACアドレスは6バイトで表示されます。

Type: エントリのタイプを示します。静的エントリはエンドユーザーが設定したものです。動的エントリは、プロセスまたはプロトコルを取得するとテーブルに追加されます。

Source:マルチキャスト転送データベースでこのエントリに対応するコンポーネント。値は、IGMP Snooping、GMRP、およびStatic Filteringとなります。

Description: マルチキャストテーブルエントリのテキスト記述

Interfaces: 転送 (Fwd:) およびフィルタリング (Flt:) に指定されているインタフェイスのリスト

Forwarding Interfaces: すべてのコンポーネントの転送インターフェイスを結合し、静的フィルタリングインタフェイスとして列記されたインタフェイスを削除し、結果転送リストが作成されます。

9.4.2.8 show mac-address-table stats

このコマンドによりMFDB統計データを表示します。

Syntax
show mac-address-table stats

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Max MFDB Table Entries: MFDBにあるエントリの合計数を示します。

Most MFDB Entries Since Last Reset: マルチキャスト転送データベーステーブルにあったエントリの最大数を示します。この値はMFDBのピーク値といいます。

Current Entries: マルチキャスト転送データベーステーブルの現在のエントリ数を示します。

9.4.3 IGMP / MLDスヌーピング

9.4.3.1 Showコマンド

9.4.3.1.1 show igmpsnooping

このコマンドによりIGMP / MLDスヌーピング情報を表示します。IGMPスヌーピングが有効かどうかの設定情報を表示します。IGMPスヌーピングが有効の場合のみ、ステータス情報が表示されます。

Syntax
show igmpsnooping [<uplinkSetName>]

<uplinkSetName> - 表示するアップリンクセット名

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Uplink Set Name: アップリンクセット名を示します。

Igmp snooping: IGMPスヌーピングの管理モードを示します。

9.4.3.2 設定コマンド

9.4.3.2.1 igmpsnooping

アップリンクセットおよび関連グループのigmpスヌーピング機能を有効化します。

Syntax
igmpsnooping <uplinkSetName> no igmpsnooping <uplinkSetName>

<uplinkSetName> - 設定するアップリンクセット名

no –特定のアップリンクセットにはIGMPスヌーピングを無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.4.4 ポートチャネル

9.4.4.1 show port-channel

このコマンドによりデバイスのすべてのダウンリンクポートチャネル (LAG) の静的機能と各ポートチャネルの概要を表示します。

Syntax
show port-channel

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Static Capability: デバイスの静的機能が有効であるかを示します。

各ポートチャネルでは、以下の情報が表示されます:

Logical Interface: 論理スロットおよび論理ポートを示します。

Port-Channel Name: ポートチャネル名を示します。

Link State: リンクがアップであるかダウンであるかを示します。

Mbr Ports: ポートチャネルのメンバーであるポートを、スロット/ポートの表記で列記します。

Active Ports: ポートチャネルにアクティブに参加しているポートを列記します。

このコマンドによりIBPのすべてのダウンリンクポートチャネル (LAG) の概要を表示します。

Syntax
show port-channel {<slot/port> | all}

<slot/port> - ポートチャネルのインタフェイス番号

all – すべてのポートチャネルのインタフェイス

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Log. Intf: 論理スロットと論理ポート

© 2010 富士通テクノロジー・ソリューションズ

Port-Channel Name: ポートチャネル (LAG) 名。最大15文字の英数字を入力できます。

Link : リンク・ステータス - リンクがアップかダウンかを示す。

Admin Mode/管理モード: 有効化または無効化します。 デフォルト設定は有効化されている。

Link Trap Mode: リンクステータスを変更した場合、トラップを送信するかを設定します。 デフォルト設定は有効化されている。

Mbr Ports: ポートチャネル (LAG) のメンバーであるポートをスロット／ポートの表記で列記します。指定ポートチャネル (LAG) には最大8つのポートを割り当てることができます。

Port Speed: ポートチャネルのポートの速度。

Type: 指定のポートチャネル (LAG) を静的または動的に管理するかを設定するステータスを示します。値は、ポートチャネルを静的に管理する場合はStatic、動的に管理する場合はDynamicとなります。

Port Active: ポートチャネル (LAG) にアクティブに参加するポートを列記します。

9.4.4.2 show lacp

このコマンドによりIBPのすべてのアップリンクセットの静的機能を表示します。

Syntax
show lacp [<uplinkSetName>]

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Uplink Set Name: アップリンクセット名を示します。

LACP: アップリンクセットのポートチャネルで静的機能が有効であるかを示します。

9.4.4.3 show lacp interface

このコマンドにより特定のインタフェイスまたはすべてのインタフェイスのLACP状態の概要を表示します。

Syntax
show lacp interface {<slot/port> | all}

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Intf: インタフェイス番号を示します。

Role: インターフェイスの役割。以下のいずれかとなります。

- Actor: LACPネゴシエーションに参加するローカルデバイス
- Partner: LACPネゴシエーションに参加するリモートデバイス

Exp: 期限切れの状態。Yesはactorまたはpartnerが期限切れの状態であることを示します。Noはactorまたはpartnerが期限切れの状態ではないことを示します。

Def: デフォルト。Yesはactorの受信マシンがデフォルトの動作partnerの情報を使用しており、partnerについて管理設定していることを示します。Noは使用している動作partnerの情報をLACP PDUで受信していることを示します。

Dist: 送信フレームの提供。Noはリンクへの送信フレーム提供が現在無効であり、有効化できないことを示します。それ以外の場合、値はYesとなります。

Col: 受信フレームの取得。Yesはリンクへの受信フレーム取得が現在有効であり、無効化できないことを示します。それ以外の場合、値はNoとなります。

Syn: 同期。Yesの場合、リンクは「同期中」となります。正しいリンク集約グループへ割り当てられ、該当する集約にグループが関連付けられ、リンク集約グループがシステムIDおよび送信された動作キー情報と照合されます。Noの場合、リンクは現在「非同期」となり、正しい集約でないことを示します。

Aggr: 集約化ポートへの集約が可能である(Yes)か、個別リンクでのみ動作する(No)かを示します。

Timeout: LACPタイムアウト設定。指定されたLACPタイムアウト設定により、低速または高速の送信レートでLACP PDUの定期送信が行われます(Long TimeoutまたはShort Timeout)。

Activity: actorまたはpartnerのポート動作。Passiveはpartnerの制御値がActiveでない場合LAC PDUの送信を行わないことを示します。Activeはpartnerの制御値に関係なくプロトコルに参加することを示します。

9.4.4.4 port-channel

このコマンドにより新規ポートチャネル (LAG) を設定し、その論理スロット番号と論理ポート番号を作成します。

注記: ポートチャネルにポートを追加する前に、ポートの物理モードを設定してください。詳細については「speed-duplex」コマンドを参照してください。

Syntax
port-channel <name> no port-channel {<slot/port> | all}

<logical slot/port> - ポートチャネルのインタフェイス番号

<name> - ポートチャネル名 (最大15文字の英数字)

all - すべてのポートチャネルのインタフェイス

no - ポートチャネルを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

Command Usage/コマンドの用法

ユーザーが作成できるポートチャネルの最大数は64、1ポートチャネルあたりの最大メンバー数は8です。

9.4.4.5 port-channel adminmode all

このコマンドによりすべての設定ポートチャネルに同じ管理モード設定を適用します。

Syntax
port-channel adminmode all no port-channel adminmode all

no - このコマンドでポートチャネル (LAG) を無効化します。すべての設定ポートチャネルに同じ管理モード設定を適用します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.4.4.6 port-channel linktrap

このコマンドによりポートチャネル (LAG) のリンクトラップ通知を有効化します。設定ポートチャネルで、インタフェイスは論理スロットおよび論理ポートとなります。allオプションではすべての設定ポートチャネルに同じ管理モード設定を適用できます。

Syntax
port-channel linktrap {<slot/port> | all} no port-channel linktrap {<slot/port> | all}

<slot/port> - ポートチャネルのインタフェイス番号

all - すべてのポートチャネルのインタフェイス

no - このコマンドによりポートチャネル (LAG) のリンクトラップ通知を無効化します。設定ポートチャネルで、インターフェイスは論理スロットおよび論理ポートとなります。allオプションによりすべての設定ポートチャネルに同じ管理モード設定を適用できます。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.4.4.7 port-channel name

このコマンドによりポートチャネル (LAG) 名を定義します。設定ポートチャネルで、インターフェイスは論理スロットおよび論理ポートとなり、名前は最大15文字の英数字となります。このコマンドによりポートチャネル作成時にそのポートチャネルに関連する名前を修正します。

Syntax
port-channel name {<slot/port> | all} <name>

<slot/port> - ポートチャネルのインタフェイス番号

all - すべてのポートチャネルのインタフェイス

<name> -設定ポートチャネル名 (最大15字)

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.4.4.8 port-channel load-balance

このCLIのコマンドで、すべてのポートチャネルの負荷分散モードを設定します。パラメータsrc-mac | dst-mac | dst-src-mac | src-ip | dst-ip| dst-src-ipは、ポートチャネルの負荷分散設定に使用するモードを示します。

Syntax
port-channel load-balance all { src-mac| dst-mac | dst-src-mac | src-ip | dst-ip| dst-src-ip } no port-channel load-balance all

src-mac - 送信元MACアドレスにモードを設定します。

dst-mac - モードを送信先MACアドレスに設定する。

dst-src-mac - モードを送信元と送信先MACアドレスに設定する。

src-ip - モードを送信元IPアドレスに設定する。

dst-ip - モードを送信先IPアドレスに設定する。

dst-src-ip - モードを送信元と送信先IPアドレスに設定する。

no - モードをデフォルト値に戻します。

初期設定

dst-src-ip

コマンド・モード

グローバル・コンフィグ

9.4.4.9 adminmode

このコマンドによりポートチャネル (LAG) のメンバーを有効化します。設定ポートチャネルで、インターフェイスは論理スロットおよび論理ポートとなります。

Syntax
adminmode no adminmode

no - このコマンドにより設定ポートチャネル (LAG) を無効化します

初期設定

有効

コマンド・モード

インターフェイス・コンフィグ

9.4.4.10 staticcapability

このコマンドにより静的ポートチャネル (静的リンク集約：LAG) のサポートを有効化します。デフォルトではすべてのポートチャネルの静的機能は無効化されています。設定ポートチャネルで、インターフェイスは論理スロットおよび論理ポートとなります。

Syntax
staticcapability no staticcapability

no - このコマンドにより静的ポートチャネルのサポートを無効化します。

初期設定

無効

コマンド・モード

インターフェイス・コンフィグ

9.4.4.11 lacp

このコマンドにより特定のアップリンクセットのリンク集約制御プロトコル (LACP) を有効化します。

Syntax
lacp <uplinkSetName> no lacp <uplinkSetName>

<uplinkSetName> - 設定するアップリンクセット名

no - このコマンドにより特定のアップリンクセットのリンク集約制御プロトコル (LACP) を無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

9.4.4.12 channel-group

このコマンドによりポートチャネル (LAG) にポートを1個追加します。最初のインターフェイスは設定ポートチャネルの論理スロット番号および論理ポート番号となります。

注記: ポートチャネルにポートを追加する前に、ポートの物理モードを設定してください。詳細については「speed-duplex」コマンドを参照してください。

Syntax
channel-group <slot/port>

<slot/port> - ポートチャネルのインタフェイス番号

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

Command Usage/コマンドの用法

ポートチャネル1個あたりの最大メンバー数は6です。

© 2010 富士通テクノロジー・ソリューションズ

9.4.4.13 delete-channel-group

このコマンドによりポートをポートチャネル (LAG) から削除します。インターフェイスは、設定ポートチャネルの論理スロット番号および論理ポート番号となります。

Syntax
delete-channel-group <slot/port>

<slot/port> - ポートチャネルのインタフェイス番号

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべての設定ポートをポートチャネル (LAG) から削除します。インターフェイスは、設定ポートチャネルの論理スロット番号および論理ポート番号となります。

Syntax
delete-channel-group <slot/port> all

<slot/port> - ポートチャネルのインタフェイス番号

all -特定のポートチャネルのすべてのメンバー

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.4.5 L2 プライオリティ

9.4.5.1 show queue cos-map

このコマンドにより特定のインターフェイスにおけるサービス優先度マップのクラスを表示します。

Syntax
show queue cos-map [<slot/port>]

<slot/port> - インターフェイス番号

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

User Priority: マップされる802.1pプライオリティを表示する。

Traffic Class: 該当する802.1pプライオリティをマップする内部トラフィッククラスを示します。

9.4.5.2 queue cos-map

このコマンドによりCoS優先度キューにサービス (CoS) 値のクラスを割り当てます。

Syntax
queue cos-map <priority> <queue-id> no queue cos-map

<queue-id> - CoS優先度キューのキューID (範囲：0～7)

<priority> - キューIDにマップするCoS値 (範囲：0～7)

no - CoSマップをデフォルト値に戻します。

初期設定

プライオリティ	キュー
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.4.6 ポートミラー

9.4.6.1 show port-monitor session

このコマンドにより特定セッションのポート監視情報を表示します。

Syntax
show port-monitor session <SessionNum>

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Session ID: セッションIDを示します。

Admin Mode/管理モード: ポート監視機能が有効であるか無効であるかを示します。値はenabledまたはdisabledとなります。

Dest. Port: ターゲットポートとして設定されているスロット／ポート。この値が設定されていない場合は'Not Configured'と表示されます。

Sour. Port: ソースポートとして設定されているスロット／ポート。この値が設定されていない場合は'Not Configured'と表示されます。

Type: ポートミラーに設定されているソースポートの方向。送信パケットの場合はtx、受信パケットの場合はrxとなります。

9.4.6.2 port-monitor session

このコマンドにより監視セッション (ポート監視) にプローブポートおよび監視先ポートを設定します。ソースインターフェイスの<slot/port>パラメータを使用して、監視元のインターフェイスを指定します。受信パケットのみの監視にはrx、送信パケットのみの監視にはtxを使用します。{rx | tx}オプションを指定していない場合、ターゲットポートで受信パケットと送信パケットの両方を監視します。ターゲットインターフェイスの<slot/port>パラメータを使用してインターフェイスを指定し、監視先のトラフィックを受信します。

Syntax
port-monitor session <session-id> {source interface <slot/port> [{rx | tx}] | destination interface <slot/port> } no port-monitor session <session-id> { source interface <slot/port> | destination interface <slot/port>}

<slot/port> - インターフェイス番号

tx/rx – 受信パケットまたは送信パケットを監視します。

no - このコマンドによりプローブポートまたはミラーポートを監視セッション (ポート監視) から削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドにより設定されたすべてのターゲットポートおよびソースポートを削除します。

Syntax
no port-monitor

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.4.6.3 port-monitor session mode

このコマンドにより監視セッションにおいてポート監視機能の管理モードを設定します。

Syntax
port-monitor session <session-id> mode no port-monitor session <session-id> mode

<session-id> - セッションID

no - このコマンドにより監視セッションについてポート監視機能を無効化します。

© 2010 富士通テクノロジー・ソリューションズ

9.5 管理コマンド

9.5.1 ネットワークコマンド

9.5.1.1 show ip interface

このコマンドによりIBPネットワークインターフェイスに関連する設定を表示します。ネットワークインターフェイスは論理インターフェイスであり、IBPのフロントパネルポートを経由し、IBPとのインバンド接続に使用されます。IBPネットワークインターフェイスに関連する設定パラメータは、トラフィックの切り替えまたはルートを行うフロントパネルポートの設定には影響を与えません。

Syntax
show ip interface

初期設定

なし

コマンド・モード

ユーザ Exec, 特権 Exec

表示メッセージ

IP Address/IPアドレス: インターフェイスのIPアドレス 工場側デフォルト設定値は0.0.0.0である。

netmask: インターフェイスのIPサブネットマスク。 工場側デフォルト設定値は0.0.0.0である。

VLAN: 管理VLAN IDを指定します。

9.5.1.2 show ip redirects

このコマンドによりIBPのIPデフォルトゲートウェイを表示します。

Syntax
show ip redirects

初期設定

なし

コマンド・モード

ユーザ Exec, 特権 Exec

表示メッセージ

IP default gateway: IPインターフェイスのデフォルトゲートウェイ。工場側デフォルト設定値は0.0.0.0である。

9.5.1.3 show ip filter

このコマンドにより管理IPフィルターステータスおよびすべての指定管理ステーションを表示します。

Syntax
show ip filter

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Index: ステーション番号

IP Address/IPアドレス: IBPの設定変更が許可されたステーションのIPアドレス

9.5.1.4 mtu

このコマンドにより物理インターフェイスとポートチャネル (LAG) インターフェイスの最大送信単位 (MTU) のサイズ (バイト単位) を設定します。標準の実装では1518～9216の範囲の有効整数である<1518-9216>となります。

Syntax
mtu <1518-9216> no mtu

<1518-9216> -最大フレームサイズ (範囲: 1518 - 9216).

no - このコマンドによりインターフェイスのデフォルト最大送信単位 (MTU) のサイズ (バイト単位) を設定します。

初期設定

1518

コマンド・モード

インターフェイス・コンフィグ

9.5.1.5 IP Address/IPアドレス

このコマンドによりIPアドレスおよびサブネットマスクを設定します。IPアドレスおよびゲートウェイは、同じサブネット上である必要があります。

Syntax
ip address <ipaddr> <netmask> <vlanid> no ip address

<ipaddr> - IP Address/IPアドレス

<netmask> - サブネットマスク

<vlanid> - VLAN ID (範囲: 1 - 4094).

no - IPアドレスおよびサブネットマスクをデフォルト値に戻します。

初期設定

IP Address/IPアドレス : 0.0.0.0

Subnet Mask : 0.0.0.0

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

Command Usage / コマンドの用法

IPアドレスを設定すると、VLAN IDの値が管理VLANに割り当てられます。

9.5.1.6 ip default-gateway

このコマンドによりデフォルトゲートウェイのIPアドレスを設定します。

Syntax
ip default-gateway <gateway> no ip default-gateway

< gateway > - デフォルトゲートウェイのIPアドレス

no - デフォルトゲートウェイのIPアドレスをデフォルト値に戻します。



インバンドおよびout-of-band (oob) の管理インターフェイスのゲートウェイを一度に設定できません。先にout-of-bandのゲートウェイ設定を行っている場合、インバンド管理インターフェイスのゲートウェイ設定を行う前にそのout-of-bandのゲートウェイ設定を削除する必要があります。

初期設定

IP Address/IPアドレス ：0.0.0.0

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.1.7 ip address protocol

このコマンドにより使用するネットワーク設定プロトコルを指定します。この値を変更すると、その変更内容が即時に適用されます。

Syntax
ip address protocol {bootp | dhcp | none}

<bootp> - BOOTPからIPアドレスを取得します。

<dhcp> - DHCPからIPアドレスを取得します。

<none> - 設定を行い、IPアドレスを取得します。



インバンドおよびout-of-bandの管理インターフェイス両方で、DHCPを使用して一度にIPアドレスをDHCPサーバから取得するよう設定できます。ただし、同時に取得できません。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.1.8 enable ip filter

このコマンドによりIPフィルタ機能を有効化します。

Syntax
ip filter no ip filter

no – IPフィルタ機能を無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

9.5.1.9 ip filter

このコマンドによりIPアドレスのフィルタ設定を行います。

Syntax
ip filter <ipaddr> no ip filter <ipaddr>

<ipaddr> - フィルタ設定を行うIPアドレスを設定します。

no -設定したフィルタIPアドレスを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.1.10 show oob

このコマンドによりout-of-band (OOB) インターフェイスに関連する設定を表示します。

Syntax
show oob

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

IP Address/IPアドレス: インターフェイスのIPアドレス 工場側デフォルト設定値は0.0.0.0である。

Subnet Mask: インターフェイスのIPサブネットマスク。 工場側デフォルト設定値は0.0.0.0である。

Default Gateway: デフォルト・ゲートウェイのIPアドレス

IPv6 Address: OOBインターフェイスのIPv6アドレス

OOB interface Configured Protocol: 使用するネットワーク設定プロトコル。 デフォルト設定はDHCPである。

Burned In MAC Address: OOBインターフェイスのデフォルトMACアドレス

9.5.1.11 oob ip

このコマンドによりIPアドレス、およびoobインターフェイスのサブネットマスクを設定します。IPアドレスおよびゲートウェイは、同じサブネット上である必要があります。

Syntax
oob ip <ipaddr> <netmask>

<ipaddr> - IP Address/IPアドレス

<netmask> - サブネットマスク

初期設定

IP Address/IPアドレス ：0.0.0.0

サブネットマスク ：0.0.0.0

コマンド・モード

グローバル・コンフィグ

9.5.1.12 oob gateway

このコマンドによりout-of-bandインターフェイスのデフォルトゲートウェイのIPアドレスを設定します。

Syntax
oob gateway <gateway> no oob gateway

< gateway > - デフォルトゲートウェイのIPアドレス

no - デフォルトゲートウェイのIPアドレスをデフォルト値に戻します。



インバンドおよびout-of-band (oob) の管理インターフェイスのゲートウェイを一度に設定できません。先にout-of-bandのゲートウェイ設定を行っている場合、インバンド管理インターフェイスのゲートウェイ設定を行う前にそのout-of-bandのゲートウェイ設定を削除する必要があります。

初期設定

Gateway Address : 0.0.0.0

コマンド・モード

グローバル・コンフィグ

9.5.1.13 oob protocol

このコマンドにより使用するoob設定プロトコルを指定します。この値を変更すると、その変更内容が即時に適用されます。

Syntax
oob protocol {bootp | dhcp | dhcp6 | none}

<bootp> - BOOTPからIPアドレスを取得します。

<dhcp> - DHCPからIPアドレスを取得します。

<dhcp6> - IPv6アドレスをDHCPv6から取得します。

<none> - 設定を行い、IPアドレスを取得します。



インバンドおよびout-of-bandの管理インターフェイス両方で、DHCPを使用して一度にIPアドレスをDHCPサーバから取得するよう設定できます。ただし、同時に取得できません。

初期設定

DHCP

コマンド･モード

グローバル･コンフィグ

© 2010 富士通テクノロジー･ソリューションズ

9.5.2 シリアルインターフェイスコマンド

9.5.2.1 show line console

このコマンドによりIBPのシリアル通信設定を表示します。

Syntax
show line console

初期設定

なし

コマンド・モード

ユーザ Exec, 特権 Exec

表示メッセージ

Serial Port Login Timeout (minutes): IBPが接続を切断したあとシリアルポート接続が動作停止となる時間を分単位で指定します。数値の範囲は0～160です。 デフォルト値は5である。0の値はタイムアウトを無効化します。

Baud Rate: シリアルポートが接続を試行するボーレートのデフォルト値。使用できる値は1200、2400、4800、9600、19200、38400、57600、115200ボーです。

Character Size: 一文字のビット数。 ビット数はつねに8となります。

Flow Control: ハードウェアフロー制御が有効であるか無効であるかを示します。ハードウェアフロー制御はつねに無効化されます。

Stop Bits: 一文字毎のストップビット数。 ストップビットは1です。

Parity: シリアルポートで使用されるパリティーの方法。 パリティーメソッドは常にNoneです。

Password Threshold: インバンドTelnetセッションの管理モード この値を無効化に設定するとTelnetポートを遮断する。 管理モードが無効化されていると、すべての既存のTelnet接続が切断される。 デフォルト値は有効である。

Silent Time (sec): パスワード閾値コマンドにより設定された閾値を失敗したログオン試行回数が超過した後、管理コンソールにアクセス不能になるまでの時間をこのコマンドで設定する。

© 2010 富士通テクノロジー・ソリューションズ

9.5.2.2 line console

このコマンドにより行設定モードに入ります。

Syntax
line console

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.2.3 baudrate

このコマンドにより端末インターフェイスの通信速度を指定します。サポートされる速度は1200、2400、4800、9600、19200、38400、57600、115200です。

Syntax
baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200} no baudrate

no - このコマンドにより端末インターフェイスの通信速度を9600に設定します。

初期設定

9600

コマンド・モード

ラインコンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.2.4 exec-timeout

このコマンドによりコンソール最大無動作接続時間 (分単位) を指定します。0の値は、コンソールが無期限に接続できることを示します。時間の範囲は0～160分です。

Syntax
exec-timeout <0-160>

<0-160> -最大接続時間 (範囲：0～160)

no - このコマンドによりコンソール最大無動作接続時間 (分単位) を5に設定します。

初期設定

5

コマンド・モード

ラインコンフィグ

9.5.2.5 password-threshold

このコマンドによりパスワード不正によるログイン失敗時の、パスワード入力制限数を設定します。

Syntax
password-threshold <0-120> no password-threshold

<threshold> -最大閾値 (範囲：0～120)

no - このコマンドにより最大値をデフォルト値に設定します。

初期設定

3

コマンド・モード

ラインコンフィグ

9.5.2.6 silent-time

このコマンドにより所定回数以上ログインに失敗した場合に管理コンソールがアクセス不可となる時間を設定します。

Syntax
silent-time <0-65535>

<0-65535> -秒単位のサイレント時間(範囲： 0 - 65535) in seconds.

no - このコマンドにより最大値をデフォルト値に設定します。

初期設定

0

コマンド･モード

ラインコンフィグ

9.5.2.7 login local

このコマンドによりログイン時のパスワード確認を有効化します。

Syntax
login local

初期設定

無効化

コマンド･モード

ラインコンフィグ

9.5.2.8 terminal-length

このコマンドによりCLIコンソール端末の長さを設定します。

Syntax
terminal-length <10-100> no terminal-length

<length> -最大閾値(範囲： 10 - 100).

no - このコマンドにより長さをデフォルト値に設定します。

初期設定

24

コマンド・モード

ラインコンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.2.9 show pager

このコマンドによりページャー設定を表示します。

Syntax
show pager

初期設定

なし

コマンド・モード

特権 Exec

9.5.2.10 pager

このコマンドによりペイジャーモードを有効化／無効化します。ページャーモードが有効の場合、データは端末上で1ページに表示されます。

Syntax
pager no pager

no - このコマンドによりページャーモードを無効に設定します。

初期設定

有効化

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.5.2.11 show displaymode

このコマンドにより拡張表示設定を表示します。

Syntax
show displaymode

初期設定

なし

コマンド･モード

特権 Exec

9.5.2.12 displaymode

このコマンドにより拡張表示モードを有効／無効化します。拡張表示モードで、1行あたり80文字以上の情報が表示されます。

Syntax
displaymode no displaymode

no - このコマンドにより拡張表示モードを無効に設定します。



拡張表示モードで情報を正しく表示するには、1行あたり80文字以上の表示に対応した端末を使用する必要があります。

初期設定

有効化

コマンド･モード

特権 Exec

© 2010 富士通テクノロジー･ソリューションズ

9.5.3 Telnetセッションコマンド

9.5.3.1 telnet

このコマンドによりリモートホストへの新規アウトバウンドtelnet接続を作成します。

Syntax
telnet <host> [port] [debug] [line] [echo]

<host> - ホスト名または有効なIPアドレス

[port] - 0～65535の範囲の有効な10進法の整数。デフォルト値は23

[debug] - 現在有効となっているtelnetオプションを表示します。

[line] - アウトバウンドtelnet動作モードをlinemodeに設定します。デフォルトの動作モードはcharacter modeです。

[echo] - ローカルエコーを有効化します。

初期設定

なし

コマンド・モード

ユーザ Exec, 特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.5.3.2 show line vty

このコマンドによりtelnetの設定を表示します。

Syntax
show line vty

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Remote Connection Login Timeout (minutes): ログオフ前にリモート接続セッションが動作停止する時間を分単位で示します。ゼロはタイムアウトがないことを示します。0～160の数を指定できます。デフォルト値は5である。

Maximum Number of Remote Connection Sessions: 許可される同時リモート接続セッション数を示します。デフォルト値は5である。

Allow New Telnet Sessions: noに設定されている場合、新規telnetセッションが許可されないことを示します。デフォルト値はyesです。

Password Threshold: ログオン試行の回数限度にコンソール・ポートで到達すると、システム・インターフェイスは次のログオン試行を許可するまでは所定時間応答を止める。 (silent time コマンドでこの間隔を設定する。) Telnetでこの閾値に到達するとTelnetのログオン・インターフェイスは閉じる。

9.5.3.3 line vty

このコマンドによりvty (Telnet) 設定モードに入ります。

Syntax
line vty

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.3.4 server enable

このコマンドによりtelnetサーバを有効または無効化します。

Syntax
server enable no server enable

no - このコマンドで無効に設定します。

初期設定

有効化

コマンド・モード

Line Vty

9.5.3.5 exec-timeout

このコマンドによりリモート接続セッションタイムアウトの値を分単位で設定します。設定した時間中にセッションがアイドル状態であれば、そのセッションはアクティブとなります。0の値はセッションが無期限にアクティブとなることを示します。時間は0～160の10進法の値です。

Syntax
exec-timeout <1-160> no exec-timeout

<sec> -最大接続時間(範囲： 1 -160).

no - このコマンドによりリモート接続セッションタイムアウトの分単位の値をデフォルト値に設定します。



アクティブセッションのタイムアウト値の変更は、そのセッションに再度アクセスすると適用されます。または、いずれかのキーを押すと新しいタイムアウト値が適用されます。

初期設定

5

コマンド・モード

Line Vty

© 2010 富士通テクノロジー・ソリューションズ

9.5.3.6 password-threshold

このコマンドによりパスワード不正によるログイン失敗時の、パスワード入力制限数を設定します。

Syntax
password-threshold <0-120> no password-threshold

<threshold> -最大閾値(範囲： 0 - 120).

no - このコマンドにより最大値をデフォルト値に設定します。

初期設定

3

コマンド・モード

Line Vty

9.5.3.7 maxsessions

このコマンドにより確立できるリモート接続セッションの最大数を指定します。0の値は、リモート接続が確立できないことを示します。範囲は0～5です。

Syntax
maxsessions <0-5> no maxsessions

<0-5> -最大セッション数(範囲： 0 - 5).

no - このコマンドにより最大値を5に設定します。

初期設定

5

コマンド・モード

Line Vty

© 2010 富士通テクノロジー・ソリューションズ

9.5.3.8 sessions

このコマンドにより新規telnetセッションを調整します。セッションが有効の場合、使用可能なセッションがそれ以上ない場合に新規telnetセッションを確立できます。セッションが無効の場合、新規telnetセッションを確立できません。確立したセッションは、終了するまで、または異常ネットワークエラーにより終了されるまでアクティブとなります。

Syntax
sessions no sessions

no - このコマンドによりtelnetセッションを無効化します。セッションが無効の場合、新規telnetセッションを確立できません。

初期設定

有効

コマンド・モード

Line Vty

9.5.3.9 terminal-length

このコマンドによりCLI vty端末の長さを設定します。

Syntax
terminal-length <10-100> no terminal-length

<length> -最大閾値(範囲： 10 - 100).

no - このコマンドにより長さをデフォルト値に設定します。

初期設定

24

コマンド・モード

Line Vty

9.5.3.10 telnet sessions

このコマンドにより新規アウトバウンドtelnet接続を調整します。有効の場合、新規アウトバウンドtelnetセッションは、許可される同時アウトバウンドtelnetセッションの最大数に到達するまで確立できます。無効の場合、新規アウトバウンドtelnetセッションを確立できません。確立したセッションは、終了するまで、または異常ネットワークエラーにより終了されるまでアクティブとなります。

Syntax
telnet sessions no telnet sessions

no - このコマンドにより新規アウトバウンドtelnet接続を無効化します。無効の場合、新規アウトバウンドtelnet接続を確立できません。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.5.3.11 telnet maxsessions

このコマンドにより同時アウトバウンドtelnetセッションの最大数を指定します。0の値は、アウトバウンドtelnetセッションを確立できないことを示します。

Syntax
telnet maxsessions <0-5> no maxsessions

<0-5> -最大セッション数(範囲： 0 - 5).

no - このコマンドにより最大値を5に設定します。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.5.3.12 telnet exec-timeout

このコマンドによりアウトバウンドtelnetセッションのタイムアウト値を分単位で設定します。

Syntax
telnet exec-timeout <1-160> no telnet exec-timeout

<1-160> - 最大接続時間(範囲： 1 -160).

no - このコマンドにより分単位のリモート接続セッションのタイムアウト値をデフォルト値に設定します。



アクティブセッションのタイムアウト値の変更は、そのセッションに再度アクセスすると適用されます。または、いずれかのキーを押すと新しいタイムアウト値が適用されます。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.5.3.13 show telnet

このコマンドにより現在のアウトバウンドtelnet設定を表示します。

Syntax
show telnet

初期設定

なし

コマンド・モード

ユーザ Exec, 特権 Exec

表示メッセージ

Outbound Telnet Login Timeout (in minutes): ログオフするまでアウトバンドtelnetセッションが動作停止となる分単位の時間を示します。0の値はデフォルト値であり、タイムアウトにならないことを示します。

Maximum Number of Outbound Telnet Sessions: 許可される同時アウトバウンドtelnet接続数を示します。

Allow New Outbound Telnet Sessions: アウトバウンドtelnetセッションを許可するかを示します。

9.5.4 SNMPサーバコマンド

9.5.4.1 show snmp

このコマンドによりSNMPコミュニティー情報を表示します。

6つのコミュニティーをサポートします。コミュニティーを追加、変更、削除できます。変更を適用するためにIBPのリセットを行う必要はありません。

IBPのSNMPエージェントは、SNMPバージョン1、2c、3に対応しています（SNMPの仕様についてはSNMP RFCを参照してください）。SNMP設定（トラップレシーバーおよびその他のSNMPコミュニティーパラメータ）に従い、TCP/IPを経由してSNMPエージェントから外部SNMPマネージャへトラップが送信されます。

Syntax
show snmp

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

SNMP Community Name/ SNMP コミュニティー名: エントリがアクセスを許可するコミュニティー名。有効なエントリは、大文字と小文字で区別される最大16文字の英数字です。テーブルの各列には固有のコミュニティー名を付ける必要があります。

Client IP Address/クライアントIPアドレス: デバイスが関連コミュニティーのSNMPパケットを受信するIPアドレス（またはその一部）。要求エンティティのIPアドレスは、そのIPアドレスとの比較前にサブネットマスクとANDされます。注記：サブネットマスクが0.0.0.0に設定されている場合、0.0.0.0のIPアドレスはすべてのIPアドレスと一致します。デフォルト値は0.0.0.0です。

Client IP Mask/クライアントIPマスク: IPアドレスとの比較前に要求エンティティのIPアドレスとANDされるマスク。結果がIPアドレスと一致すると、そのアドレスは認証済みIPアドレスとなります。例えば、IPアドレスが9.47.128.0、対応サブネットマスクが255.255.255.0の場合、受信IPアドレスの範囲が一致します。つまり、受信IPアドレスは9.47.128.0 - 9.47.128.255と同等となります。デフォルト値は0.0.0.0です。

Access Mode/アクセス・モード: コミュニティー文字列のアクセスレベル

Status/ステータス： コミュニティーアクセスエントリのステータス

© 2010 富士通テクノロジー・ソリューションズ

9.5.4.2 show trapflags

このコマンドによりトラップ条件を表示します。トラップ条件を有効化ないし無効化し、IBPが作成するトラップを設定します。トラップ条件が有効の場合に条件が検出されると、IBPのSNMPエージェントからすべての有効なトラップレシーバーへトラップが送信されます。変更を適用させるためにIBPのリセットを行う必要はありません。コールドスタートおよびウォームスタートのトラップがつねに作成されるようになっており、この設定を無効化できません。

Syntax
show trapflags

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Authentication Flag: 有効化または無効化します。 デフォルト設定は有効化されている。認証失敗トラップを送信するかを示します。

Link Up/Down Flag: 有効化または無効化します。 デフォルト設定は有効化されている。リンクステータストラップを送信するかを示します。

Multiple Users Flag: 有効化または無効化します。 デフォルト設定は有効化されている。ユーザーIDが一度に複数回IBPにログインした場合、トラップを送信するかを示します (Telnetまたはシリアルポート経由) 。

ACL Traps: 有効化または無効化します。 工場側デフォルトは無効化されている。 ACLトラップを送信するかを示します。

9.5.4.3 snmp-server sysname

このコマンドによりIBP名を設定します。名前の範囲は1～31文字の英数字です。

Syntax
snmp-server sysname <name>

<name> -名前の範囲は1～31文字の英数字です。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.4.4 snmp-server location

このコマンドによりIBPの場所を設定します。名前の範囲は1～31文字の英数字です。

Syntax
snmp-server location <loc>

<loc> - 名前の範囲は1～31文字の英数字です。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.4.5 snmp-server contact

このコマンドによりネットワーク責任者を設定します。範囲は1～31文字の英数字です。

Syntax
snmp-server contact <con>

<con> - 名前の範囲は1～31文字の英数字です。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.4.6 snmp-server community

このコマンドにより新規SNMPコミュニティーを追加し、名前を与えます。コミュニティー名は IBP、および特定権限レベルで管理を行うSNMPマネージャに関連する名前となります。名前の長さは大文字と小文字で区別される最大16文字です。

注記: SNMPコミュニティーテーブルのコミュニティー名は固有のものである必要があります。同じコミュニティー名を使用し複数のエントリを作成した場合、最初のエントリが保持および処理され、その他の重複エントリは無視されます。

Syntax
snmp-server community <name> no snmp-server community <name>

<name> - コミュニティー名 (大文字と小文字で区別される最大16文字)

no – このコマンドによりこのコミュニティー名をテーブルから削除します。名前は削除するコミュニティー名となります。

初期設定

publicおよびprivateの2つのデフォルトコミュニティー名。このデフォルトコミュニティー名を、コミュニティーごとに固有の識別子に変更できます。残りの4つのコミュニティー名のデフォルト値は空欄となっています。

コマンド・モード

グローバル・コンフィグ

このコマンドによりSNMPコミュニティーをアクティブにします。コミュニティーが有効の場合、このコミュニティーのSNMPマネージャはアクセス権に従いIBPを管理します。コミュニティーが無効の場合、このコミュニティーを使用したSNMP要求は拒否されます。この場合、このコミュニティーのSNMPマネージャは、ステータスが有効に設定されるまで、IBPを管理できません。

Syntax
snmp-server community mode <name> no snmp-server community mode <name>

<name> - コミュニティー名

no - このコマンドによりSNMPコミュニティーを非アクティブ化します。コミュニティーが無効の場合、このコミュニティーを使用したSNMP要求は拒否されます。この場合、このコミュニティーのSNMPマネージャは、ステータスが有効に設定されるまで、IBPを管理できません。

初期設定

publicおよびprivateのコミュニティーはデフォルトで有効化されています。また、定義されていない4つのコミュニティーはデフォルトで無効化されています。

コマンド・モード

グローバル・コンフィグ

このコマンドによりSNMPコミュニティーにクライアントIPマスクを設定します。アドレスは、関連コミュニティーのSNMPパケット送信アドレスであり、デバイスへのアクセス時にSNMPクライアントがコミュニティーを使用できるIPアドレスの範囲を示す、クライアントIPアドレスの値とともに使用されます。255.255.255.255の値で1ステーションからのアクセスを許可し、クライアントIPアドレスのマシンIPアドレスを使用します。0.0.0.0の値ですべてのIPアドレスからのアクセスを許可します。名前は、該当するコミュニティー名となります。

Syntax
snmp-server community ipmask <ipmask> <name> no snmp-server community ipmask <name>

<name> - コミュニティー名

<ipmask> - クライアントIPマスク

no - このコマンドによりSNMPコミュニティーのクライアントIPマスクを0.0.0.0に設定します。名前は、該当するコミュニティー名となります。 コミュニティー名には最大16文字の英数字を使用できます。

初期設定

0.0.0.0

コマンド・モード

グローバル・コンフィグ

このコマンドによりIBP情報へのアクセスを制限します。アクセスモードは読み取り専用 (public) または読み書き可 (private) です。

Syntax
snmp-server community {ro | rw} <name>

<name> - コミュニティー名

<ro> - アクセスモードは読み取り専用

<rw> - アクセスモードは読み書き可

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.4.7 snmp-server host

このコマンドによりSNMPコミュニティーのクライアントIPアドレスを設定します。アドレスは、関連コミュニティーのSNMPパケット送信アドレスであり、デバイスへのアクセス時にSNMPクライアントがコミュニティーを使用できるIPアドレスの範囲を示す、クライアントIPマスク値とともに使用されます。0.0.0.0の値ですべてのIPアドレスからのアクセスを許可します。クライアントIPアドレスのマシンIPアドレスを使用します。0.0.0.0の値ですべてのIPアドレスからのアクセスを許可します。それ以外の場合、この値はマスクとANDされ、許可するクライアントIPアドレスの範囲が決定されます。名前は、該当するコミュニティー名となります。

Syntax
snmp-server host <ipaddr> <name> No snmp-server host <name>

<name> - コミュニティー名

<ipaddr> - クライアントIPアドレス

no - このコマンドによりSNMPコミュニティーのクライアントIPアドレスを0.0.0.0に設定します。 名前は、該当するコミュニティー名となります。

初期設定

0.0.0.0

コマンド・モード

グローバル・コンフィグ

9.5.4.8 snmp-server enable traps

このコマンドによりACLトラップを有効化します。

Syntax
snmp-server enable traps acl-trapflags no snmp-server enable traps acl-trapflags

no - このコマンドによりACLトラップを無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

このコマンドにより認証トラップを有効化します。

Syntax
snmp-server enable traps authentication no snmp-server enable traps authentication

no - このコマンドにより認証トラップを無効化します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

このコマンドによりIBP全体のLink Up/Downトラップを有効化します。有効の場合、およびポートに関連するLink Trapフラグ設定が有効の場合のみリンクトラップが送信されます（**snmp trap link-status**コマンドを参照してください）。

Syntax
snmp-server enable traps linkmode no snmp-server enable traps linkmode

no - このコマンドによりIBP全体のLink Up/Downトラップを無効化します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

このコマンドによりMultiple Userトラップを有効化します。トラップが有効の場合、およびユーザーが端末インターフェイス（EIA 232またはtelnet）にログインし、現在端末インターフェイスセッションがある場合に、Multiple Userトラップが送信されます。

Syntax
snmp-server enable traps multiusers no snmp-server enable traps multiusers

no - このコマンドによりMultiple Userトラップを無効化します。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.5 SNMPトラップコマンド

9.5.5.1 show snmptrapコマンド

このコマンドによりSNMPトラップレシーバーを表示します。トラップメッセージはネットワークを経由しSNMPネットワークマネージャへ送信されます。このメッセージで、IBP内またはネットワーク上で発生したイベントをマネージャに通知します。同時に6つのトラップレシーバーに対応します。

Syntax
show snmptrap

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

SNMP Trap Name: トラップマネージャへ送信されるSNMPトラップパケットのコミュニティー名。最大16文字の英数字を使用できます。文字列は大文字、小文字で区別されます。

IP Address/IPアドレス: SNMPトラップをデバイスから受信するIPアドレス。0から255までの4個の数字をピリオドで区切り入力する。

SNMP Version: レシーバーが使用するトラップバージョン

SNMP v1 - SNMP v1を使用し、レシーバーへトラップを送信

SNMP v2 - SNMP v2を使用し、レシーバーへトラップを送信

ステータス： レシーバーのステータス（有効または無効）を示し、管理者／ユーザーによるこのユーザーエントリへの動作を許可するプルダウンメニュー

有効化 - レシーバーへトラップを送信する

無効化- レシーバーへトラップを送信しない

© 2010 富士通テクノロジー・ソリューションズ

9.5.5.2 snmp trap link-status

このコマンドによりインターフェイスのリンクステータストラップを有効化します。

注記：このコマンドはLink Up/Downフラグが有効な場合のみ、有効化されます。**snmp-server enable traps linkmode**コマンドを参照してください。

Syntax
snmp trap link-status no snmp trap link-status

no - このコマンドによりインターフェイスのリンクステータストラップを無効化します。

初期設定

無効化

コマンド・モード

インターフェイス・コンフィグ

このコマンドによりすべてのインターフェイスのリンクステータストラップを有効化します。

注記: このコマンドはLink Up/Downフラグが有効な場合のみ、有効化されます（**snmp-server enable traps linkmode**コマンドを参照してください）。

Syntax
snmp trap link-status all no snmp trap link-status all

all - すべてのインターフェイス。

no - このコマンドによりすべてのインターフェイスのリンクステータストラップを無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.5.3 snmptrap <name> <ipaddr>

このコマンドによりSNMPトラップ名を追加します。名前は大文字と小文字で区別される最大16文字の英数字です。

Syntax
snmptrap <name> <ipaddr> no snmptrap <name> <ipaddr>

<name> - SNMPトラップ名 (範囲:大文字と小文字で区別される最大16文字の英数字)

<ipaddr> - トラップレシーバーのIPアドレス

no - このコマンドでコミュニティーのトラップレシーバーを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.5.4 snmptrap ipaddr

このコマンドにより特定コミュニティー名のトラップレシーバーのIPアドレスを変更します。名前は大文字と小文字で区別される最大16文字の英数字です。.

注記:SNMPトラップレシーバーテーブルのIPアドレスは、同じコミュニティー名で固有のものである必要があります。同じIPアドレスおよびコミュニティー名を使用し複数のエントリを作成した場合、最初のエントリが保持および処理され、その他の重複エントリは無視されます。

Syntax
snmptrap ipaddr <name> <ipaddr> <ipaddrnew>

<name> - SNMPトラップ名

<ipaddr> - 元のIPアドレス

<ipaddrnew> - 新規IPアドレス

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.5.5 snmptrap mode

このコマンドによりSNMPトラップをアクティブ化または非アクティブ化します。有効なトラップレシーバーはアクティブ化され（トラップ受信可）、無効なトラップレシーバーは非アクティブ化され（トラップ受信不可）ます。

Syntax
snmptrap mode <name> <ipaddr> no snmptrap mode <name> <ipaddr>

<name> - SNMPトラップ名

<ipadd> - IPアドレス

no - このコマンドによりSNMPトラップを非アクティブ化します。トラップレシーバーは非アクティブ化します（トラップを受信できません）。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.5.6 snmptrap snmpversion

このコマンドによりSNMPトラップをアクティブ化または非アクティブ化します。有効なトラップレシーバーはアクティブ化され（トラップ受信可）、無効なトラップレシーバーは非アクティブ化され（トラップ受信不可）ます。

Syntax
snmptrap snmpversion <name> <ipaddr> <snmpv1|snmpv2>

<name> - SNMPトラップ名

<ipadd> - IPアドレス

snmpv1 - SNMP v1を使用し、トラップを送信

Snmpv2 - SNMP v3を使用し、トラップを送信

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.6 HTTPコマンド

9.5.6.1 show ip http

このコマンドによりIBPのhttp設定を表示します。

Syntax
show ip http

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

HTTP Mode (Unsecure): HTTPモードが有効であるか無効であるかを示します。

HTTP Port: HTTPに設定されているポートを示します。

HTTP Mode (Secure): セキュアHTTPの管理モードが有効であるか無効であるかを示します。

Secure Port: セキュアHTTPに設定されているポートを示します。

Secure Protocol Level(s): プロトコルレベルはSSL3、TSL1、またはSSL3とTSL1両方のいずれかの値となります。

9.5.6.2 ip javamode

このコマンドによりIBPがWebインターフェイスのヘッダーフレームのJavaアプレットへのアクセスを許可するかを指定します。アクセスが有効の場合、ユーザーはWebインターフェイスからJavaアプレットを閲覧できます。アクセスが無効の場合、Javaアプレットを閲覧できません。

Syntax
ip javamode no ip javamode

no - このコマンドによりWebインターフェイスのヘッダーフレームのJavaアプレットへのアクセスを許可しません。javaモードが無効の場合、ユーザーはJavaアプレットを閲覧できません。

初期設定

有効化

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.6.3 ip http port

このコマンドによりhttpポートを1-65535に設定します。デフォルトのポートは80です。

Syntax
ip http port <1-65535> no ip http port

<1-65535> - HTTPポート値

no - このコマンドによりhttpポートをデフォルト値にリセットします。

初期設定

80

コマンド・モード

グローバル・コンフィグ

9.5.6.4 ip http server

このコマンドによりWebインターフェイスを経由したIBPへのアクセスを有効化します。アクセスが有効な場合、ユーザーはWebインターフェイスからIBPへログインできます。アクセスが無効の場合、ユーザーはIBPのWebサーバへログインできません。

Webインターフェイスを無効にすると即時にすべてのインターフェイスに適用されます。

Syntax
ip http server no ip http server

no - このコマンドによりWebインターフェイスを経由したIBPへのアクセスを無効化します。アクセスが無効の場合、ユーザーはIBPのWebサーバへログインできません。

初期設定

有効

コマンド・モード

グローバル・コンフィグ

9.5.6.5 ip http secure-port

このコマンドによりセキュアHTTPポートを1-65535に設定します。デフォルトのポートは443です。

Syntax
ip http secure-port <portid> no ip http secure-port

<portid> - セキュアHTTPポート値

no - このコマンドによりセキュアHTTPポートをデフォルト値にリセットします。

初期設定

443

コマンド･モード

グローバル･コンフィグ

9.5.6.6 ip http secure-server

このコマンドによりセキュアHTTPのセキュアソケットレイヤーを有効化します。

Syntax
ip http secure-server no ip http secure-server

no - このコマンドによりセキュアHTTPのセキュアソケットレイヤーを無効化します。

初期設定

無効

コマンド･モード

グローバル･コンフィグ

9.5.6.7 ip http secure-protocol

このコマンドによりプロトコルレベル (バージョン) を設定します。プロトコルレベルはTLS1、SSL3、またはTLS1とSSL3両方のいずれかに設定できます。

Syntax
ip http secure-protocol <protocollevel1> [protocollevel2] no ip http secure-protocol <protocollevel1> [protocollevel2]

<protocollevel1 - 2> - プロトコルレベルはTLS1、SSL3、またはTLS1とSSL3両方のいずれかに設定できます。

no - このコマンドによりセキュアHTTPのプロトコルレベル (バージョン) を削除します。

初期設定

SSL3 と TLS1

コマンド・モード

グローバル・コンフィグ

9.5.6.8 ip http session

このコマンドによりhttp hard-timeout、maxsessions、およびsoft-timeoutのパラメータを設定します。

Syntax
ip http session { hard-timeout <0-168> | maxsessions <0-16> | soft-timeout <0-60> } no ip http session { hard-timeout | maxsessions | soft-timeout }

hard-timeout <0-168>: HTTPセッションのハードタイムアウト (時間単位) を設定します。

maxsessions <0-16>: HTTPセッションの最大許可数を設定します。

soft-timeout <0-60>: HTTPセッションのソフトタイムアウト (分単位) を設定します。

no - このコマンドによりHTTPセッションのパラメータをデフォルト値に戻します。

初期設定

maxsessions: 16

hard-timeout: 24

soft-timeout: 15

コマンド・モード

グローバル・コンフィグ

9.5.6.9 ip http secure-session

このコマンドによりhttp hard-timeout、maxsessions、およびsoft-timeoutのパラメータを設定します。

Syntax
ip http secure-session { hard-timeout <0-168> | maxsessions <0-16> | soft-timeout <0-60> } no ip http secure-session { hard-timeout | maxsessions | soft-timeout }

hard-timeout <0-168>: セキュアHTTPセッションのハードタイムアウト (時間単位) を設定します。

maxsessions <0-16>: セキュアHTTPセッションの最大許可数を設定します。

soft-timeout <0-60>: セキュアHTTPセッションのソフトタイムアウト (分単位) を設定します。

no - このコマンドによりセキュアHTTPセッションのパラメータをデフォルト値に戻します。

初期設定

maxsessions: 16

hard-timeout: 24

soft-timeout: 5

コマンド・モード

グローバル・コンフィグ

9.5.7 セキュアShell (SSH) コマンド

9.5.7.1 show ip ssh

このコマンドによりSSH設定を表示します。

Syntax
show ip ssh

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Administrative Mode: SSHの管理モードが有効であるか無効であるかを示します。

Protocol Levels: プロトコルレベルはversion 1、version 2、あるいは両方のバージョンとなります。

SSH Sessions Currently Active: 現在のSSH接続数を示します。

Max SSH Sessions Allowed: IBPで許可されるインバウンドSSHセッションの最大数を示します。

SSH Timeout: IBPの受信SSHセッションの不動作タイムアウト値を示します

9.5.7.2 ip ssh

このコマンドによりSSH設定を表示します。

Syntax
ip ssh no ip ssh

no - このコマンドによりSSHを無効化します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

9.5.7.3 ip ssh protocol

このコマンドによりSSHのプロトコルレベル（またはバージョン）を設定または削除します。SSH1 (1)、SSH2 (2)、あるいはSSH 1とSSH 2 (1 と 2) 両方のいずれかに設定できます。

Syntax
ip ssh protocol <protocollevel1> [protocollevel2]

<protocollevel1 - 2> - プロトコルレベルはSSH1、SSH2、あるいはSSH 1とSSH 2両方のいずれかに設定できます。

初期設定

SSH1 と SSH2

コマンド・モード

グローバル・コンフィグ

9.5.7.4 ip ssh maxsessions

このコマンドにより作成できるSSH接続セッションの最大数を指定します。0の値はssh接続を作成できないことを示します。範囲は0～5です。

Syntax
ip ssh maxsessions <0-5> no ip ssh maxsessions

<0-5> - セッションの最大数

no - このコマンドにより作成できるSSH接続セッションの最大数をデフォルト値に戻します。

初期設定

5

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.7.5 ip ssh timeout

このコマンドによりSSH接続セッションタイムアウト値を分単位で設定します。セッションが指定時間中アイドル状態であれば、そのセッションはアクティブとなります。0の値はセッションが無期限にアクティブとなることを示します。時間の整数値の範囲は0〜160です。アクティブセッションのタイムアウト値の変更は、そのセッションに再度アクセスすると適用されます。または、いずれかのキーを押すと新しいタイムアウト値が適用されます。

Syntax
ip ssh timeout <1-160> no ip ssh timeout

<1-160> -秒単位のタイムアウト間隔

no - このコマンドにより分単位のSSH接続セッションタイムアウト値をデフォルト値に戻します。 アクティブセッションのタイムアウト値の変更は、そのセッションに再度アクセスすると適用されます。または、いずれかのキーを押すと新しいタイムアウト値が適用されます。

初期設定

5

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.8 DHCPクライアントコマンド

9.5.8.1 ip dhcp restart

このコマンドによりBOOTPまたはDHCPのクライアント要求を開始します。

Syntax
ip dhcp restart

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.5.8.2 ip dhcp client-identifier

このコマンドによりこのIBPのDHCPクライアント識別子を指定します。noを使用すると、デフォルト値に戻ります。

Syntax
ip dhcp client-identifier {text <text> | hex <hex>} no ip dhcp client-identifier

<text> - テキスト文字列(範囲： 1-15 characters).

<hex> - XX:XX:XX:XX:XX:XX (Xは0～9、A～F) 形式の16進数文字列

no - このコマンドによりデフォルト値に戻ります。



接続ブレードのMMBまたはCLIからホスト名が変更されると、DHCPクライアント識別子も変更されます。

初期設定

CB.SerialNumber

コマンド・モード

グローバル・コンフィグ

9.5.9 DHCPv6クライアントコマンド

9.5.9.1 ipv6 address protocol

このコマンドにより使用するIPv6設定プロトコルのネットワークを指定します。この値を変更すると、その変更内容が即時に適用されます。

Syntax
ipv6 address protocol {dhcp6 | none}

<dhcp6> - DHCPv6からIPアドレスを取得します。

<none> - 設定を行い、IPアドレスを取得します。

初期設定

なし.

コマンド・モード

インターフェイス-VLANコンフィグ

9.5.9.2 ipv6 dhcp6 restart

このコマンドによりネットワークインターフェイスからのDHCPv6クライアント要求を開始します。

Syntax
ipv6 dhcp6 restart

初期設定

なし.

コマンド・モード

グローバル・コンフィグ

9.5.9.3 oob protocol

このコマンドにより使用するoob設定プロトコルを指定します。この値を変更すると、その変更内容が即時に適用されます。

Syntax
oob protocol {bootp | dhcp | dhcp6 | none}

<bootp> - BOOTPからIPアドレスを取得します。

<dhcp> - DHCPからIPアドレスを取得します。

<dhcp6> - IPv6アドレスをDHCPv6から取得します。

<none> - 設定を行い、IPアドレスを取得します。

初期設定

DHCP.

コマンド・モード

グローバル・コンフィグ

9.5.9.4 oob protocol dhcp6 restart

このコマンドによりoobインターフェイスからのDHCPv6クライアント要求を開始します。

Syntax
oob protocol dhcp6 restart

初期設定

なし.

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.10 ドメインネームサーバリレーコマンド

9.5.10.1 Showコマンド

9.5.10.1.1 show hosts

このコマンドにより静的ホストのネーム-アドレスマッピングテーブルを表示します。

Syntax
show hosts

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Domain Name List/ドメイン・ネーム・リスト: ドメイン名

IP Address/IPアドレス: ホストのIPアドレス

9.5.10.1.2 show dns

このコマンドによりDNSサーバの設定を表示します。

Syntax
show dns

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Domain Lookup Status: IPドメインネームシステム (DNS) ベースのホストのネームーアドレス変換機能を有効または無効化します。

Default Domain Name: ホストのIPアドレスのクエリに使用するデフォルトのドメイン名

Domain Name List/ドメイン・ネーム・リスト: ホストのIPアドレスのクエリに使用するドメイン名のリスト

Name Server List: ドメインネームサーバのリスト

© 2010 富士通テクノロジー・ソリューションズ

Request/要求 ： 送信されたDNSクエリパケットの数

Response: 受信されたDNS応答パケットの数

9.5.10.2 show dns cache

このコマンドによりDNSキャッシュテーブルにあるすべてのエントリを表示します。

Syntax
show dns cache

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Domain Name List/ドメイン・ネーム・リスト: ドメイン名

IP Address/IPアドレス: 該当するドメイン名のIPアドレス

TTL: このエントリがDNSキャッシュテーブルに保持される秒単位の時間

Flag/フラグ: このエントリの信頼性を示します。例:8の値は10の値より信頼性はありません。

9.5.10.3 設定コマンド

9.5.10.3.1 ip hosts

このコマンドによりIPアドレスにホスト名をマップするDNSテーブルに、静的エントリを作成します。

Syntax
ip host <name> <ipaddr> no ip host <name>

<name> - ホスト名

<ipaddr> - ホストのIPアドレス

<no> - IPアドレスのマッピングエントリから該当する名前を削除します。

初期設定

なし

コマンド・モード

特権 Exec

9.5.10.3.2 clear hosts

このコマンドにより静的ホスト全体のネーム-アドレスマッピングテーブルをクリアします。

Syntax
clear hosts

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.5.10.3.3 ip domain-name

このコマンドにより不完全なホスト名（クライアントから送信されたホスト名に「.」が使用されていない場合）に付与するデフォルトのドメイン名を定義します。

Syntax
ip domain-name <name> no ip domain-name <name>

<name> - 未認定のホスト名を完了させるために使用されるデフォルト・ドメイン名 未認定の名前をドメイン名から分離する初期フェーズは含めないこと。 (範囲: 1-64 文字)

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.5.10.3.4 ip domain-list

このコマンドにより不完全なホスト名（クライアントから送信されたホスト名に「.」が使用されていない場合）に付与するドメイン名を定義します。ドメイン名テーブルには最大6エントリを含めることができます。

Syntax
ip domain-list <name> no ip domain-list <name>

<name> - 未認定のホスト名を完了させるために使用されるデフォルト・ドメイン名 未認定の名前をドメイン名から分離する初期フェーズは含めないこと。 (範囲： 1-64文字)



不完全なホスト名をIBP上のDNSサーバから受信した場合、ドメイン名リストを使用しリスト内の各ドメイン名がホスト名に付与され、一致する名前のサーバがないか確認されます。ドメイン名リストがない場合は、*ip domain-name*コマンドで指定されたドメイン名が使用されます。 ドメイン名リストがある場合は、デフォルトのドメイン名は使用されません。

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.5.10.3.5 ip name-server

このコマンドによりネームアドレス解決に使用する複数のドメインネームサーバのアドレスを指定します。ドメインネームサーバテーブルには最大6エントリを含めることができます。

Syntax
ip name-server <ipaddr> no ip name-server <ipaddr>

< ipaddr > - ドメインネームサーバのIPアドレス

<no> -該当するドメインネームサーバエントリをテーブルから削除します。



列記されたネームサーバは、応答を受信するまで、あるいはリストの最後まで応答がない場合に、指定シーケンスでクエリされます。

初期設定

なし

コマンド・モード

特権 Exec

9.5.10.3.6 ip domain-lookup

このコマンドによりIPドメインネームシステム (DNS) ベースのホストのname-to-address変換を有効化します。

Syntax
ip domain-lookup no ip domain-lookup

<no> - このコマンドによりIPドメインネームシステム (DNS) ベースのホストのname-to-address変換を無効化します。

初期設定

なし

コマンド・モード

特権 Exec

9.5.10.3.7 clear domain-listコマンド

このコマンドによりドメイン名リストテーブルのすべてのエントリをクリアします。

Syntax
clear domain-list

初期設定

なし

コマンド・モード

特権 Exec

9.5.10.3.8 clear dns

このコマンドによりDNSをデフォルト値に戻します。

Syntax
clear dns

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.5.10.3.9 clear dns cache

このコマンドによりDNSキャッシュテーブルのすべてのエントリをクリアします。

Syntax
clear dns cache

初期設定

なし

コマンド・モード

特権 Exec

9.5.10.3.10 clear dns counter

このコマンドによりDNSキャッシュテーブルのすべてのエントリの統計データをクリアします。

Syntax
clear dns cache

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.5.11 動的DNSクライアントコマンド

9.5.11.1 ddns client

このコマンドによりddnsプロバイダがドメインレコードを更新したことを通知するためのDDNS (動的DNS) 更新を行います。更新が成功した場合、ddnsリストにそのパラメータが保存されます。

動的DNSは、IPルータやコンピュータシステムなどのインターネットプロトコルスイートを使用しネットワーク上のデバイスに機能を提供する、メソッド、プロトコル、あるいはネットワークサービスです。設定ホスト名、アドレス、またはDNSに保存されているその他の情報のアクティブDNS設定の変更について、ドメインネームサーバへリアルタイムに通知を行います。

Syntax
ddns { dhs | dyndns | dyns | easydns | ods | tzo | zoneedit } <username> <password> <host> [<address>] no ddns { dhs | dyndns | dyns | easydns | ods | tzo | zoneedit } <username> <password> <host> [<address>]

<no> - このコマンドによりddns設定をリストから削除します。

初期設定

なし.

コマンド・モード

グローバル・コンフィグ

9.5.11.2 show ddns

このコマンドによりDDNS設定リストを表示します。

Syntax
Show ddns

初期設定

なし.

コマンド・モード

特権 Exec

表示メッセージ

Server Name: DDNSサーバのプロバイダ名

User Name: DDNSサーバのユーザー名

Password: アカウントのパスワード

Host: IPアドレスでマップするドメイン名

IP Address/IPアドレス: ドメイン名でマップするIPアドレス

9.5.12 IPv6コマンド

9.5.12.1 show ipv6 interface

このコマンドによりIBPのIPv6ネットワーク設定を表示します。

Syntax
show ipv6 interface

初期設定

なし.

コマンド・モード

ユーザ Exec, 特権 Exec

表示メッセージ

IPv6 Address/IPv6アドレス: インターフェイスのIPv6アドレス

Address mode/アドレスモード: 使用するIPv6プロトコルのネットワーク設定。デフォルト値はNone.

9.5.12.2 show ipv6 traffic

このコマンドによりIPv6 and ICMPv6のトラフィックおよび統計データを表示します。インターフェイスを指定し、そのトラフィック情報を閲覧できます。

Syntax
show ipv6 traffic {oob | switchport}

初期設定

なし.

コマンド・モード

ユーザ Exec, 特権 Exec

表示メッセージ

Total Datagrams Received: インターフェイスで受信した、エラーを含む入力データグラムの合計数

Received Datagrams Locally Delivered: IPv6ユーザープロトコル (ICMPを含む) に正しく送信されたデータグラムの合計数。このカウンタはこのデータグラムが宛てられたインターフェイスでインクリメントします。データグラムによっては入力インターフェイスとは限りません。

Received Datagrams Discarded Due To Header Errors: バージョン番号不一致、その他の形式エラー、ホップカウント超過、IPv6オプション処理中のエラー検出などを含むIPv6ヘッダーのエラーにより破棄された、入力データグラムの数。

Received Datagrams Discarded Due To MTU: サイズが送信インターフェイスのリンクMTUのサイズを超過したため送信できなかった、入力データグラムの数。

Received Datagrams Discarded Due To No Route: 宛先に送信するルートが見つからなかったため破棄された、入力データグラムの数。

Received Datagrams With Unknown Protocol: 正しく受信したが、不明または非対応プロトコルのため破棄された、ローカルでアドレスされたデータグラムの数。このカウンタはこのデータグラムが宛てられたインターフェイスでインクリメントします。データグラムによっては入力インターフェイスとは限りません。

Received Datagrams Discarded Due To Invalid Address: IPv6ヘッダーの宛先フィールドのIPv6アドレスが、このエンティティで受信できる有効アドレスでないため破棄された、入力データグラムの数。このカウントには、無効なアドレス（::0など）や非対応アドレス（割り当てられていない接頭辞のあるアドレスなど）が含まれます。IPv6ルーターではないためデータグラムを転送しないエンティティについては、このカウンターはターゲット・アドレスがローカル・アドレスでなかったために破棄されたデータグラムを含む。

Received Datagrams Discarded Due To Truncated Data: データグラムフレームに十分なデータがないため破棄された、入力データグラムの数。

Received Datagrams Discarded Other: 処理を継続できない問題はないが破棄された入力IPv6データグラムの数（例：バッファスペース不足など）。注記：このカウンタには、再取得の待機中に破棄されたデータグラムは含まれません。

Received Datagrams Reassembly Required: インターフェイスで再取得する必要のある受信IPv6断片数。注記：このカウンタはこのフラグメントが宛てられたインターフェイスでインクリメントします。フラグメントの入力インターフェイスとは限りません。

Datagrams Successfully Reassembled: 正しく再取得されたIPv6データグラムの数。注記：このカウンタはこのデータグラムが宛てられたインターフェイスでインクリメントします。フラグメントの入力インターフェイスとは限りません。

Datagrams Failed To Reassemble: IPv6再取得アルゴリズムで検出された失敗数（タイムアウト、エラーなど、すべての理由による）。注記：受信時に結合されているアルゴリズム（受信アルゴリズム）もあるため、破棄されたIPv6断片数とは限りません。このカウンタはフラグメントが宛てられたインターフェイスでインクリメントします。フラグメントの入力インターフェイスとは限りません。

Datagrams Forwarded: エンティティがターゲットで送受信した出力データグラムの数。IPv6ルータとして動作しないエンティティ内では、このカウンタにはこのエンティティを経由しソースルートされたパケットのみが含まれ、ソースルート処理は成功となります。注記：データグラムの転送が成功すると、出力インターフェイスのカウンタがインクリメントします。

Datagrams Locally Transmitted: 送信要求でローカルIPv6ユーザープロトコル（ICMPを含む）によりIPv6に送信されたIPv6データグラムの合計数。注記：このカウンタにはipv6IfStatsOutForwDatagramsのデータグラムは含まれません。

Datagrams Transmit Failed: 宛先へ送信できない問題はないが破棄された（バッファスペース不足など）出力IPv6データグラムの数。注記：パケットがこの（任意の）破棄規則に該当する場合、このカウンタにはipv6IfStatsOutForwDatagramsのデータグラムは含まれません。

Fragments Created: 出力インターフェイスのフラグメントにより作成された出力データグラムフラグメント数。

Datagrams Successfully Fragmented: 出力インターフェイスで正しくフラグメントされたIPv6データグラムの数。

Datagrams Failed To Fragment: 出力インターフェイスでフラグメントする必要があるが失敗したため破棄されたIPv6データグラムの数。

Multicast Datagrams Received: インターフェイスで受信したマルチキャストパケットの数。

Multicast Datagrams Transmitted: インターフェイスが送信されたマルチキャストパケットの数。

合計受信ICMPv6メッセージ：ipv6IfIcmpInErrorsでカウントされた数を含む、インターフェイスで受信したICMPメッセージの合計数。注記：このインターフェイスは、ICMPメッセージが宛てられたインターフェイスであり、メッセージの入力インターフェイスであるとは限りません。

ICMPv6 Messages with errors: インターフェイスで受信しICMPの特定エラー（ICMPチェックサム、不正な長さなど）により与えられたICMPメッセージの数。

ICMPv6 Destination Unreachable Messages: インターフェイスで受信したICMP Destination Unreachableメッセージの数。

ICMPv6 Messages Prohibited Administratively: インターフェイスで受信した、管理者に禁止されるICMP destination unreachable/communicationメッセージの数。

ICMPv6 Time Exceeded Messages: インターフェイスで受信したICMP Time Exceededメッセージの数。

ICMPv6 Parameter Problem Messages: インターフェイスで受信したICMP Parameter Problemメッセージの数。

ICMPv6 messages with too big packets: インターフェイスで受信したICMP Packet Too Bigメッセージの数。

ICMPv6 Echo Request Messages Received: インターフェイスで受信したICMP Echo（要求）メッセージの数。

ICMPv6 Echo Reply Messages Received: インターフェイスで受信したICMP Echo Replyメッセージの数。

ICMPv6 Router Solicit Messages Received: インターフェイスで受信したICMP Router Solicitメッセージの数。

ICMPv6 Router Advertisement Messages Received: インターフェイスで受信したICMP Router Advertisementメッセージの数。

ICMPv6 Neighbor Solicit Messages Received: インターフェイスで受信したICMP Neighbor Solicitメッセージの数。

ICMPv6 Neighbor Advertisement Messages Received: インターフェイスで受信したICMP Neighbor Advertisementメッセージの数。

ICMPv6 Redirect Messages Received: インターフェイスで受信したRedirectメッセージの数。

ICMPv6 Group Membership Query Messages Received: インターフェイスで受信したICMPv6 Group Membership Queryメッセージの数。

ICMPv6 Group Membership Response Messages Received: インターフェイスで受信したICMPv6 group Membership Responseメッセージの数。

ICMPv6 Group Membership Reduction Messages Received: インターフェイスで受信したICMPv6 Group Membership Reductionメッセージの数。

Total ICMPv6 Messages Transmitted: インターフェイスが送信試行したICMPメッセージの合計数。注記：このカウンタにはicmpOutErrorsでカウントされたすべての数が含まれます。

ICMPv6 Messages Not Transmitted Due To Error: ICMPでバッファ不足などの問題がありインターフェイスが送信しなかったICMPメッセージの数。この値には、IPv6が結果データグラムをルートできないなどのICMPレイヤー外で検出されたエラーは含まれません。実装によってはこのカウンタ値に該当するエラータイプがない場合があります。

ICMPv6 Destination Unreachable Messages Transmitted: インターフェイスが送信したICMP Destination Unreachableメッセージの数。

ICMPv6 Messages Prohibited Administratively Transmitted: インターフェイスが送信した、管理者に禁止されるICMP destination unreachable/communicationメッセージの数。

ICMPv6 Time Exceeded Messages Transmitted: インターフェイスが送信したICMP Time Exceededメッセージの数。

ICMPv6 Parameter Problem Messages Transmitted: インターフェイスが送信したICMP Parameter Problemメッセージの数。

ICMPv6 Packet Too Big Messages Transmitted: インターフェイスが送信したICMP Packet Too Bigメッセージの数。

ICMPv6 Echo Request Messages Transmitted: インターフェイスが送信したICMP Echo（要求）メッセージの数。

ICMPv6 Echo Reply Messages Transmitted: インターフェイスが送信したICMP Echo Replyメッセージの数。

© 2010 富士通テクノロジー・ソリューションズ

ICMPv6 Router Solicit Messages Transmitted: インターフェイスが送信したICMP Router Solicitationメッセージの数。

ICMPv6 Router Advertisement Messages Transmitted: インターフェイスで受信したICMP Router Advertisementメッセージの数。

ICMPv6 Neighbor Solicit Messages Transmitted: インターフェイスが送信したICMP Neighbor Solicitationメッセージの数。

ICMPv6 Neighbor Advertisement Messages Transmitted: インターフェイスが送信したICMP Neighbor Advertisementメッセージの数。

ICMPv6 Redirect Messages Transmitted: インターフェイスが送信したRedirectメッセージの数。ホストはRedirectを送信しないため、ホストでこのオブジェクトはつねにゼロとなります。

ICMPv6 Group Membership Query Messages Transmitted: インターフェイスが送信したICMPv6 Group Membership Queryメッセージの数。

ICMPv6 Group Membership Response Messages Transmitted: インターフェイスが送信したICMPv6 group Membership Responseメッセージの数。

ICMPv6 Group Membership Reduction Messages Transmitted: インターフェイスが送信したICMPv6 Group Membership Reductionメッセージの数。

ICMPv6 Duplicate Address Detects: インターフェイスが検出した重複アドレスの数。

9.5.12.3 clear ipv6 statistics

このコマンドにより特定インターフェイスのIPv6統計データをクリアします。show ipv6 trafficコマンドの出力でIPv6統計データを表示します。

Syntax
clear ipv6 statistics {oob | switchport}

初期設定

なし.

コマンド・モード

特権 Exec

9.5.13 LLDPコマンド

9.5.13.1 show lldp

このコマンドにより現在のLLDP設定の概要を表示します。

Syntax
show lldp

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Transmit Interval: システムがローカルデータLLDPフレームを送信する間隔を秒単位で示します。

Transmit Hold Multiplier: ローカルデータLLDPフレームにTTLを設定する送信間隔のマルチプライヤを示します。

Re-initialization Delay: 再開までの遅延時間を秒単位で示します。

Notification Interval: システムがリモートデータ変更通知を送信する間隔を秒単位で示します。

9.5.13.2 show lldp interface

このコマンドにより特定インターフェイスまたはすべてのインターフェイスの現在のLLDP設定の概要を表示します。

Syntax
show lldp interface {<slot/port> | all}

<slot/port> -特定のインターフェイスを設定します。

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

インターフェイス：インターフェイスをスロット／ポートの表記で示します。

Link: リンクがupであるかdownであるかを示します。

Transmit: インターフェイスがLLDPフレームを送信するかを示します。

Receive: インターフェイスがLLDPフレームを受信するかを示します。

Notify: インターフェイスがリモートデータ変更通知を送信するかを示します。

TLVs: インターフェイスがLLDPフレームに任意のTLVを送信するかを示します。TLVコードは0 (ポート記述)、1 (システム名)、2 (システム記述)、3 (システム機能) のいずれかとなります。

Mgmt: インターフェイスがLLDPフレームにシステム管理アドレス情報を送信するかを示します。

9.5.13.3 show lldp statistics

このコマンドにより特定インターフェイスまたはすべてのインターフェイスの現在のLLDPトラフィックおよびリモートテーブル統計データを表示します。

Syntax
show lldp statistics {<slot/port> | all}

<slot/port> - 特定のインターフェイスを設定します。

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Last Update: リモートテーブルへの最終更新からの経過時間を日、時間、分、秒で示します。

Total Inserts: リモートデータテーブルへの挿入の合計数

Total Deletes: リモートデータテーブルからの削除の合計数

Total Drops: 受信した完全なリモートデータが不正リソースのため挿入されなかった合計回数

Total Ageouts: TTL間隔が期限切れのため完全なリモートデータエントリが削除された合計回数

テーブルには以下の行見出しが表示されます。

インターフェイス:インターフェイスをスロット／ポートの表記で示します。

Transmit Total: ポートに送信されたLLDPフレームの合計数

Receive Total: ポートで受信したLLDPフレームの合計数

Discards: なんらかの理由によりポートで破棄されたLLDPフレームの合計数

Errors: ポートで受信した無効LLDPフレーム数

Ageouts: Time to Live intervalが期限切れのためポートで完全なリモートデータが削除された合計回数

TLV Discards: 破棄されたTLV数

TLV Unknowns: タイプ値が制限範囲内のため認識されなかった場合の、ポートで受信したLLDP TLVの合計数

9.5.13.4 show lldp remote-device

このコマンドにより現在のLLDPデータをシステムに送信するリモートデバイスの概要情報を表示します。すべてのポートまたは特定のポートで受信したLLDPリモートデータの情報を表示できます。

Syntax
show lldp remote-device {<slot/port> | all}

<slot/port> -特定のインターフェイスを示します。

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Local Interface/ローカル・インターフェイス: リモートデバイスからLLDPフレームを受信したインターフェイスを示します。

Chassis ID /シャーシID: リモートデバイスのIDを示します。

Port ID/ポートID: LLDPフレームを送信したポート番号を示します。

System Name/システム名: リモートデバイスのシステム名を示します。

© 2010 富士通テクノロジー・ソリューションズ

9.5.13.5 show lldp remote-device detail

このコマンドにより現在のLLDPデータをシステムのインターフェイスに送信するリモートデバイスに関する詳細情報を表示します。

Syntax
show lldp remote-device detail <slot/port>

<slot/port> -特定のインターフェイスを示します。

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Local Interface/ローカル・インターフェイス: リモートデバイスからLLDPフレームを受信したインターフェイスを示します。

Chassis ID Subtype/シャーシIDサブタイプ: Chassis IDフィールドで使用されている認識タイプを示します。

Chassis ID/シャーシID: リモートデバイスのシャーシを示します。

Port ID Subtype/ポートIDサブタイプ: リモートデバイスのポートタイプを示します。

Port ID/ポートID: LLDPフレームを送信したポート番号を表示します。

System Name/システム名: リモートデバイスのシステム名を示します。

System Description/システム内容: システム名、およびデバイスでサポートされているハードウェア、OS、ネットワークソフトウェアのバージョンを識別し、リモートシステムを記述します。

Port Description/ポート内容: 英数字でポートを記述します。ポート記述は設定可能です。

System Capabilities Supported/サポートされるシステム機能: デバイスのプライマリ機能を示します。

System Capabilities Enabled/有効化されたシステム機能: 有効である対応システム機能を示します。

Management Address/管理アドレス: LLDPエージェントのあるリモートデバイスの各インターフェイスで、リモートLLDPエージェントが使用するアドレスタイプを列記し、デバイスに関連する情報を取得するアドレスを指定します。

Time To Live: LLDPフレームで受信したリモートデバイスの情報を有効な情報として処理するまでの時間 (秒単位) を示します。

9.5.13.6 show lldp local-device

このコマンドにより通知されたLLDPローカルデータに関する概要情報を表示します。各インターフェイスの概要情報または詳細情報を表示できます。

Syntax
show lldp local-device {<slot/port> | all}

<slot/port> - 特定のインターフェイスを示します。

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

インターフェイス：インターフェイスをスロット／ポートの表記で示します。

Port ID: インターフェイスに関連するポートIDを示します。

Port Description: インターフェイスに関連するポート記述を示します。

9.5.13.7 show lldp local-device detail

このコマンドにより特定のインターフェイスが送信するLLDPデータの詳細情報を表示します。

Syntax
show lldp local-device detail <slot/port>

<slot/port> - 特定のインターフェイスを示します。

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

インターフェイス：LLDPフレームを送信するインターフェイスを示します。

Chassis ID Subtype/シャーシIDサブタイプ: Chassis IDフィールドで使用されている認識タイプを示します。

Chassis ID/シャーシID: ローカルデバイスのシャーシを示します。

Port ID Subtype/ポートIDサブタイプ: ローカルデバイスのポートタイプを示します。

Port ID/ポートID: LLDPフレームを送信したポート番号を示します。

© 2010 富士通テクノロジー・ソリューションズ

System Name/システム名: ローカルデバイスのシステム名を示します。

システム内容: システム名、およびデバイスでサポートされているハードウェア、OS、ネットワークソフトウェアのバージョンを識別し、ローカルシステムを記述します。

Port Description/ポート内容: 英数字でポートを記述します。

System Capabilities Supported/サポートされるシステム機能: デバイスのプライマリ機能を示します。

System Capabilities Enabled/有効化されたシステム機能: 有効である対応システム機能を示します。

Management Address/管理アドレス: ローカルLLDPエージェントが情報の送受信に使用するアドレスタイプおよび特定のアドレスを列記します。

9.5.13.8 lldp notification

このコマンドによりリモートデータ変更通知を有効化します。

Syntax
lldp notification no lldp notification

no - このコマンドにより通知を無効化します。

初期設定

無効

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.13.9 lldp notification-interval

このコマンドによりシステムがリモートデータ変更通知を送信する間隔を設定します。<interval-seconds>パラメータは、通知送信ごとの秒単位の待機時間です。有効な間隔範囲は5～3600秒です。

Syntax
lldp notification-interval <interval-seconds> no lldp notification-interval

<interval-seconds> -通知送信ごとの待機時間を秒単位で設定します。

no - このコマンドにより通知間隔をデフォルト値に戻します。

初期設定

5

コマンド・モード

グローバル・コンフィグ

9.5.13.10 lldp receive

このコマンドによりLLDP受信機能を有効化します。

Syntax
lldp receive no lldp receive

no - このコマンドによりLLDPフレームの受信機能をデフォルト値に戻します。

初期設定

無効化

コマンド・モード

インターフェイス・コンフィグ

9.5.13.11 lldp transmit

このコマンドによりLLDPアドバタイズ機能を有効化します。

Syntax
lldp transmit no lldp transmit

no - このコマンドによりローカルデータ送信機能をデフォルト値に戻します。

初期設定

無効化

コマンド・モード

インターフェイス・コンフィグ

9.5.13.12 lldp transmit-mgmt

このコマンドによりローカルシステム管理アドレス情報をLLDP PDUに追加します。

Syntax
lldp transmit-mgmt no lldp transmit-mgmt

no - このコマンドによりLLDPフレームへの管理情報の追加をキャンセルします。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.5.13.13 lldp transmit-tlv

このコマンドによりLLDPフレームに送信する802.1AB基本管理設定の任意のタイプの長さの値 (TLV) を指定します。sys-nameを使用すると、システム名のTLVを送信します。システム名の設定方法については、snmp-serverコマンドを参照してください。sys-desctoを使用すると、システム記述のTLVを送信します。sys-capを使用すると、システム機能のTLVを送信します。port-descを使用すると、ポート記述のTLVを送信します。ポート記述の設定方法については、descriptionコマンドにより参照してください。

Syntax
lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc] no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]

no - このコマンドにより任意のTLVをLLDPフレームから削除します。パラメータのないコマンドを使用すると、すべての任意のTLVをLLDPフレームから削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.5.13.14 lldp timers

このコマンドによりLLDPが有効であるポートのローカルデータ送信のタイミングパラメータを設定します。<interval-seconds>で、ローカルデータLLDPフレームの送信ごとの待機時間を秒単位で設定します。範囲は1～32768秒です。<hold-value>は、ローカルデータLLDPフレームのTTLを設定する送信間隔のマルチプライヤを示し、範囲は2～10です。<reinit-seconds>は、再開までの遅延時間を示し、範囲は1～0秒です。

Syntax
lldp timers [interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>] no lldp timers [interval] [hold] [reinit]

<interval-seconds> - ローカルデータLLDPフレームの送信ごとの待機時間を秒単位で設定します。

<hold-value> - ローカルデータLLDPフレームにTTLを設定する転送間隔のマルチプライヤを設定します。

<reinit-seconds> -再開までの遅延時間を設定します。

no - このコマンドによりLLDPが有効であるポートのローカルデータ送信に関する、一部またはすべてのタイミングパラメータをデフォルト値に戻します。

初期設定

Interval-seconds: 30

Hold-value: 4

Reinit-seconds: 2

コマンド・モード

グローバル・コンフィグ

9.6 システムログ管理コマンド

9.6.1 Showコマンド

9.6.1.1 show loggingコマンド

このコマンドによりログを表示します。

Syntax
show logging

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Logging Client Local Port: syslogメッセージを送信するコレクタ／リレーのポート

CLI Command Logging: CLIコマンドログのモード

Console Logging: コンソールログのモード

Console Logging Severity Filter: コンソールログへログを行う重要度の最低値。この数値以下のメッセージがログされます。

Buffered Logging: バッファされたログのモード

Syslog Logging:設定されたsyslogホストにログを行うモード。無効に設定するとすべてのsyslogホストへのログが停止します。

Log Messages Received: ログプロセスで受信したメッセージ数。ドロップまたは無視されたメッセージも含まれます。

Log Messages Dropped: 処理できなかったメッセージ数

Log Messages Relayed: リレーされたメッセージ数

Log Messages Ignored: 無視されたメッセージ数

© 2010 富士通テクノロジー・ソリューションズ

9.6.2 show logging buffered

このコマンドによりIBPで保持されているメッセージログを表示します。メッセージログにはシステム追跡情報が含まれます。

Syntax
show logging buffered

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Buffered (In-Memory) Logging: メッセージログが有効であるか無効であるかを示します。

Buffered Logging Wrapping Behavior: ラッピングが有効であるか無効であるかを示します。

Buffered Log Count: ログされたメッセージ数を示します。

Message: ログされたメッセージ



メッセージログ情報は、IBPをリセットすると削除されます。

9.6.3 show logging traplog

このコマンドによりIBPで保持されているトラップログを表示します。トラップログには、ラップした最大256エントリが含まれます。

Syntax
show logging traplogs

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Number of Traps since last reset: デバイスが最後にリセットされてから発生したトラップの数

Trap Log Capacity: IBPに保存できるトラップの最大数

Log: トラップのシーケンス番号

System Up Time/システム稼働時間: トラップが発生しIBPを最後に再起動した時間

Trap: トラップの情報



トラップログ情報は、IBPをリセットすると削除されます。

9.6.3.1 show logging hosts

このコマンドによりすべての設定ログホストを表示します。

Syntax
show logging hosts

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Index (used for deleting)/ Indexコマンド(削除に使用される)

IP Address/IPアドレス: 設定サーバのIPアドレス

Severity: 特定のアドレスにログを行う重要度の最低値

Port Server Port Number: syslogメッセージを送信したローカルホストのポート

ステータス： 設定syslogホストへのログ状態。ステータスが無効の場合、ログは行われません。

© 2010 富士通テクノロジー・ソリューションズ

9.6.4 設定コマンド

9.6.4.1 logging buffered

このコマンドにより最大128ログを保存できる内部メモリログへのログ実施を有効化します。

Syntax
logging buffered no logging buffered

no - このコマンドにより内部メモリログへのログ実施を無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりログ可能最大数に到達した場合の内部メモリログのラッピングを有効化します。無効の場合、ログ可能最大数に到達するとログが停止します。

Syntax
logging buffered wrap no logging buffered wrap

no - このコマンドによりログ可能最大数に到達した場合の内部メモリログのラッピングを無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.6.4.2 logging console

このコマンドによりコンソールへのログ実施を有効化します。

Syntax
logging console [<severitylevel> | <0-7>] no logging console

[<severitylevel> | <0-7>] -緊急 (0) 、警告 (1) 、重要 (2) 、エラー (3) 、注意 (4) 、指示 (5) 、通知 (6) 、デバッグ (7) の内容で、0～7の整数で表示されます。

no - このコマンドによりコンソールへのログ実施を無効化します。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

9.6.4.3 logging host

このコマンドにより最大8つのホストを設定できる場合にホストへのログを有効化します。

Syntax
logging host <hostaddress> [<port>] [[<severitylevel> | <0-7>]]

<hostaddress> - ログサーバのIPアドレス

<port> - ポート番号

[<severitylevel> | <0-7>] -緊急 (0) 、警告 (1) 、重要 (2) 、エラー (3) 、注意 (4) 、指示 (5) 、通知 (6) 、デバッグ (7) の内容で、0～7の整数で表示されます。

初期設定

なし

コマンド･モード

グローバル･コンフィグ

© 2010 富士通テクノロジー･ソリューションズ

このコマンドによりホストへのログ実施を無効化します。

Syntax
logging host remove <hostindex>

<hostindex> - ログサーバのインデックス

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりログサーバのIPアドレスを再設定します。

Syntax
logging host reconfigure <hostindex> {host <hostaddress> | port <port> | severitylevel <level>}

<hostindex> - ログサーバのIPアドレス

host -新規ログホストのIPアドレスの変更

<hostaddress> - ログサーバの新規IPアドレス

port -新規ログホストのポートの変更

<port> - <1 - 65535>の範囲の新規ポート値

severitylevel -新規ログホストの重要度の変更

[<severitylevel> | <0-7>] -緊急(0)、警告(1)、重要(2)、エラー(3)、注意(4)、指示(5)、通知(6)、デバッグ(7)の内容で、0～7の整数で表示されます。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.6.4.4 logging syslogコマンド

このコマンドによりsyslogのログ実施を有効化します。

Syntax
logging syslog no logging syslog

no - syslogのログ実施を無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりログメッセージでのLOGクライアントのローカルポート数を設定します。

.

Syntax
logging syslog port <portid> no logging syslog port

no - ローカルログポートをデフォルト値に戻します。

<portid> - 1～65535のポートID

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.6.4.5 clear logging buffered

このコマンドによりすべての内部メモリログをクリアします。

Syntax
clear logging buffered

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.7 スクリプト管理コマンド

9.7.1 script apply

このコマンドにより設定スクリプトのコマンドをIBPに適用します。適用コマンドにより動作設定のバックアップを行い、スクリプトファイルへのコマンド適用を開始します。コマンド適用は、コマンドが最初に失敗した時に停止します。

Syntax
script apply <scriptname>

<scriptname> -適用するスクリプト名

初期設定

なし

コマンド・モード

特権 Exec

9.7.2 script delete

このコマンドにより特定のスクリプト、またはIBPで与えられているすべてのスクリプトを削除します。

Syntax
script delete {<scriptname> | all}

<scriptname> -削除するスクリプト名

all - IBPで与えられているすべてのスクリプトを削除します。

初期設定

なし

コマンド・モード

特権 Exec

9.7.3 script list

このコマンドによりIBP上にあるすべてのスクリプト、およびファイルの合計数を列記します。

Syntax
script list

初期設定

なし

コマンド・モード

特権 Exec



すべてのスクリプトファイルの合計サイズは2 MBを超えることはできません。

9.7.4 script show

このコマンドによりスクリプトファイルの内容を表示します。

Syntax
script show <scriptname>

<scriptname> - スクリプトファイル名

初期設定

なし

コマンド・モード

特権 Exec

9.8 システムユーティリティ

9.8.1 clear

9.8.1.1 clear arp

このコマンドにより動的タイプのすべてのARPエントリを、ARPキャッシュから削除します。

Syntax
clear arp

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.2 clear traplog

このコマンドによりトラップログをクリアします。

Syntax
clear traplog

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.1.3 clear eventlog

このコマンドによりシステムからのエラーメッセージが含まれたイベントログをクリアします。

Syntax
clear eventlog

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.4 clear logging buffered

このコマンドによりIBPで保持されているメッセージログをクリアします。メッセージログにはシステムトレース情報が含まれています。

Syntax
clear logging buffered

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.5 clear config

このコマンドによりIBPの電源をオフにせずに設定をデフォルト値にリセットします。このコマンドを実行するとIBPが自動的にリセットされます。リセット実施前に確認メッセージが表示されます。

Syntax
clear config

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.6 clear pass

このコマンドによりIBPの電源をオフにせずにすべてのユーザーパスワードをデフォルト値にリセットします。パスワードのリセット実施前に確認メッセージが表示されます。

Syntax
clear pass

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.1.7 clear counters

このコマンドにより特定の<slot/port>の統計データ、すべてのポートの統計データ、または引数に基づくIBP全体の統計データをクリアします。

Syntax
clear counters [<slot/port> | all]

<slot/port> -必要なインターフェイス番号である

all - すべてのインターフェイス。

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.8 clear dns counter

このコマンドでDNS統計データをクリアします。

Syntax
clear dns counter

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.9 clear dns cache

このコマンドによりDNSキャッシュからすべてのエントリをクリアします。

Syntax
clear dns cache

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.1.10 enable passwd

このコマンドにより特権 Execのパスワードを変更します。

Syntax
enable passwd {0 | 7} <password>

0 - プレーンテキストのパスワードを示します。

7 - 暗号化形式のパスワードを示します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.8.1.11 clear igmp snooping

このコマンドによりIGMPスヌーピング機能で管理されているテーブルをクリアし、マルチキャスト転送データベースからそのエントリの削除を試行します。

Syntax
clear igmp snooping

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.1.12 clear mld snooping

このコマンドによりMLDスヌーピング機能で管理されているテーブルをクリアし、マルチキャスト転送データベースからそのエントリの削除を試行します。

Syntax
clear mld snooping

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.13 clear port-channel

このコマンドによりすべてのポートチャネル (LAG) をクリアします。

Syntax
clear port-channel

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.14 clear port-security dynamic

このコマンドによりすべてのポートセキュリティ動的情報をクリアします。

Syntax
clear port-security dynamic {address <mac-addr> | interface <slot/port>}

address - MACアドレスの動的アドレスをクリアします。

<mac-addr> - MACアドレス

interface - インターフェイスの動的アドレスをクリアします。

<slot/port> -必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.15 clear ip filter

このコマンドによりすべてのipフィルターエントリをクリアします。

Syntax
clear ip filter

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.16 clear ipv6 statistics

このコマンドによりIPv6統計データをリセットします。

Syntax
clear ipv6 statistics {oob | switchport}

oob - アウトバウンドのIPv6統計データをクリアします。

switchport - インバウンドのIPv6統計データをクリアします。

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.1.17 clear dot1x statistics

このコマンドにより特定のポートまたはすべてのポートの802.1x統計データをリセットします。

Syntax
clear dot1x statistics {all | <slot/port>}

<slot/port> - 必要なインターフェイス番号である。

all - すべてのインターフェイス。

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.18 clear radius statistics

このコマンドによりすべてのRADIUS統計データをクリアします。

Syntax
clear radius statistics

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.1.19 clear tacacs

このコマンドによりTACACS+設定をクリアします。

Syntax
clear tacacs

初期設定

なし

コマンド・モード

特権 Exec

9.8.1.20 clear lldp

このコマンドによりLLDP統計データをクリアします。

Syntax
clear lldp {remote-data | statistics}

remote-data - lldpリモートデータをクリアします。

statistics - lldp統計データをクリアします。

初期設定

なし

コマンド・モード

特権 Exec

9.8.2 copy

このコマンドによりIBPへ(から)アップロードおよびダウンロードを行います。ローカルURLは、tftpまたはxmodemを使用して指定できます。IBPからアップロードを行うソースファイルに、開始設定(startup-config)、イベントログ(eventlog)、メッセージログ(msglog)、トラップログ(traplog)を指定できます。宛先はURLで指定されます。

このコマンドによりURLにソース、および開始設定またはイメージに宛先を指定し、開始設定またはコードイメージをダウンロードできます。

このコマンドにより動作設定にソース、および開始設定{*filename*}に宛先を指定し、動作設定をフラッシュメモリに保存できます。

また、このコマンドによりsshkey-rsa、sshkey-rsa2、sshkey-dsaのsshキーファイル、またsslpem-root、sslpem-server、sslpem-dhweak、sslpem-dhstrongのhttpセキュアサーバ証明書をダウンロードできます。

9.8.2.1 PCへのファイルのアップロード

Syntax
copy startup-config <sourcefilename> <url> copy {errorlog | log | traplog} <url> copy script <sourcefilename> <url> copy image <filename> <url> where <url>={xmodem | tftp://ipaddr/path/file | ftp://user:pass@ipaddr/path/file}

<sourcefilename> -設定ファイルまたはスクリプトファイルのファイル名

<url> - xmodem or tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.

errorlog - イベントのログファイル

log - メッセージのログファイル

traplog - トラップのログファイル

<filename> -設定ファイル名またはイメージファイル名

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.2.2 PCからスイッチへダウンロードされるファイル

Syntax
copy <url> startup-config <destfilename> copy <url> image <destfilename> copy <url> {sshkey-rsa1 | sshkey-rsa2 | sshkey-dsa} copy <url> {sslpem-root | sslpem-server | sslpem-dhweak | sslpem-dhstrong} copy <url> script <destfilename> where <url>={xmodem | tftp://ipaddr/path/file | ftp://user:pass@ipaddr/path/file}

<destfilename> - イメージファイル名またはスクリプトファイル名

<url> - xmodem or tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.

sshkey-rsa1 - SSH RSA1キーファイル

sshkey-rsa2 - SSH RSA2キーファイル

sshkey-dsa - SSH DSAキーファイル

sslpem-root - Secure Root PEMファイル

sslpem-server - Secure Server PEMファイル

sslpem-dhweak - Secure DH Weak PEMファイル

sslpem-dhstrong - Secure DH Strong PEMファイル

初期設定

なし

コマンド・モード

特権 Exec

9.8.2.3 動作設定ファイルをフラッシュメモリに書き込む

Syntax
copy running-config startup-config [filename]

<filename> -設定ファイル名

初期設定

なし

コマンド・モード

特権 Exec

9.8.2.4 事前ログインバナーファイルをアップロード、ダウンロードする

Syntax
copy clibanner <url> copy <url> clibanner no clibanner

<url> - xmodem or tftp://ipaddr/path/file or ftp://user:pass@ipaddr/path/file.

no - CLIバナーを削除します。

初期設定

なし

コマンド・モード

特権 Exec

9.8.2.5 システム設定ファイルをコピーする

Syntax
copy file running-config

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.3 delete

このコマンドにより設定ファイルまたはイメージファイルを削除します。

Syntax
delete <filename>

<filename> -設定ファイル名またはイメージファイル名

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.4 dir

このコマンドによりフラッシュメモリ上のファイルのリストを表示します。

Syntax
dir [boot-rom | config | opcode [<filename>]]

<filename> - 必要なインターフェイス番号である。

boot-rom - 起動ロム。

config -設定ファイル

opcode - ランタイム動作コード

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

列見出し	説明
date	ファイル作成日
file name	ファイル名
file type	ファイルタイプ：ブートROM、動作コード、設定ファイル
startup	システム開始時にこのファイルを使用するかを示します。
size	バイト単位のファイルの長さ

9.8.5 whichboot

このコマンドによりシステム開始時にブートしたファイルを表示します。

Syntax
whichboot

初期設定

なし

コマンド・モード

特権 Exec

表示メッセージ

Boot-System: 現在のブートモード

Next Booting Mode: リブート後のブートモード

file name: 必要なインターフェイス番号である。

file type: ブートROMイメージ、動作コード、または設定ファイル

startup: ブート時に使用します。

size (byte): 設定ファイルまたはイメージファイルのサイズ

9.8.6 boot-system

このコマンドによりシステム開始に使用するファイルまたはイメージを指定します。

Syntax
boot-system {boot-rom | config | opcode | Auto (オート) -copy-sw} <filename> boot-system mode {switch | IBP}

<filename> - 必要なインターフェイス番号である。

boot-rom - bootrom.

config - 設定ファイル

opcode - ランタイム動作コード

mode - SwitchまたはIBPに切り替えます。

(*)Auto (オート) -copy-sw - スタックシステムの自動アップグレード機能を設定します。

注記: (*)はスタッキングコマンドです。

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.7 ping

このコマンドにより別のコンピュータがネットワーク上にあり、接続に応答するかを確認します。このコマンドを使用するには、IBPをネットワーク (インバンド) 接続設定します。ソースおよび対象デバイスでpingユーティリティが有効となっており、TCP/IPの最上層で動作している必要があります。IBPとワークステーション間の物理パスがあれば、IBPがデフォルトのVLAN (VLAN 1) を経由して接続しているどのIPワークステーションからでもIBPにpingできます。端末インターフェイスから、3つのpingが対象ステーションに送信されます。

Syntax
ping <host>

<host> - ホスト名またはIPアドレス

初期設定

なし

コマンド・モード

特権 Exec

9.8.7.1 変更パラメータ値についてpingする

Syntax
ping <host> count <0-20000000> [size <32-512>] ping <host> size <32-512> [count <0-20000000>]

<host> - ホスト名またはIPアドレス

<0-20000000> - pingの数 (範囲:0～20000000) 。注記:0は無限を示します。

<size> - パケットサイズ (範囲:32～512)

初期設定

Count = 5

Size = 32

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.7.2 IPv6アドレスについてpingする

Syntax
ping ipv6 <ipv6-address>

<ipv6-address> - IPv6アドレス

初期設定

なし

コマンド・モード

特権 Exec

9.8.7.3 インターフェイスキーワードを使用するリンクローカルアドレスについてpingする

Syntax
ping ipv6 interface {oob | switchport} <link-local-address> [size <datagram-size>]

oob - out-of-bandのインターフェイス

switchport -インバンドのインターフェイス

<link-local-address> - リンクローカルアドレス

<datagram-size> - データグラムサイズ (範囲：48～2048)

初期設定

なし

コマンド・モード

特権 Exec

© 2010 富士通テクノロジー・ソリューションズ

9.8.8 traceroute

このコマンドによりパケットがホップごとにネットワーク経由で宛先に送信された際に、実際に通過するルートを確認します。<ipaddr>は有効なIPである必要があります。[port]は0～65535の範囲の有効な10進法の整数である必要があります。デフォルト値は33434です。任意のポートパラメータは、トレースルートの一部として送信されたパケットの宛先に使用される、UDPポートです。このポートは、宛先のシステム上の未使用ポートである必要があります。

Syntax
traceroute <ipaddr|hostname> [initTtl <1-255>] [maxTtl <1-255>] [interval <1-60>] [count <1-10>] traceroute ipv6 <ipv6-address> [initTtl <1-255>] [maxTtl <1-255>] [interval <1-60>] [count <1-10>]

<ipaddr|hostname> - ホスト名またはIPアドレス

initTtl - 使用する初期TTL

<1-255> - 範囲：1～255

maxTtl - 宛先の最大TTL

<1-255> - 範囲：1～255

Interval - プローブの秒単位の間隔

<1-60> - 範囲：1～60

count - 1ホップあたりのプローブ数

<1-10> - 範囲：1～10

<ipv6-address> - IPv6アドレス

初期設定

initTtl = 1

maxTtl = 20

interval = 3

count = 3

コマンド・モード

特権 Exec

9.8.9 logging cli-command

このコマンドによりCLIコマンドのログ機能を有効化します。コマンドのログコンポーネントにより、システム上で発行されたすべてのCommand Line Interface (CLI) コマンドがIBPでログされます。

Syntax
logging cli-command

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.8.10 カレンダー設定

このコマンドによりシステム時計を設定します。

Syntax
calendar set <mm/dd/yyyy> <hh:mm:ss>

<mm/dd/yyyy> - 月 (範囲：1～12) 、日 (範囲：1～31) 、年 (4桁。範囲：2000～2099)

<hh:mm:ss> - 24時間形式、hh (時間。範囲：0～23) 、mm (分。範囲：0～59) ss (秒。範囲：0～59)

初期設定

なし

コマンド・モード

特権 EXEC

9.8.11　　reload

このコマンドによりIBPの電源をオフにせずにリセットします。リセットにより、すべてのネットワーク接続が終了し、起動コードが実行されます。IBPは保存された設定を使用し、IBPを初期化します。リセット実施前に確認メッセージが表示されます。リセットが成功すると、IBP上のLEDで表示されます。

Syntax
reload [slot <unit>]

(*)slot - スタックまたはスタック内のIBPをリロードします。

(*)<unit> - 1～8のスイッチIDまたはCB名

注記：(*) はスタッキングコマンドです。

初期設定

なし

コマンド・モード

特権 EXEC

9.8.12　　構成

このコマンドによりグローバル設定モードをアクティブ化します。

Syntax
configure

初期設定

なし

コマンド・モード

特権 EXEC

9.8.13　　disconnect

このコマンドによりtelnetセッションを閉じます。

Syntax
disconnect {<0-42> | all}

<0-42> - リモートセッションID

all - すべてのリモートセッション

初期設定

なし

コマンド・モード

特権 EXEC

9.8.14 hostname

このコマンドによりプロンプト文字列を設定します。

Syntax
hostname <prompt_string>

< prompt_string > - プロンプト文字列

初期設定

CB

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.8.15 pager

このコマンドによりページャー設定を有効化／無効化します。

Syntax
pager no pager

no - このコマンドによりページャー機能を無効化します。

初期設定

なし

コマンド･モード

特権 EXEC

9.8.16 do

このコマンドによりグローバル設定モードまたは設定サブモードから特権 EXEC-levelコマンドを実行します。

© 2010 富士通テクノロジー･ソリューションズ

Syntax
do [EXEC-level command]

[EXEC-level command / EXEC-levelコマンド] - 特権 EXEC Commandモードの特権 Exec-levelコマンド

初期設定

なし

コマンド･モード

グローバル･コンフィグ、設定サブモード

9.8.17 quit

このコマンドによりCLIセッションを終了します。

Syntax
quit

初期設定

なし

コマンド･モード

特権 EXEC

9.9 ユーザアカウント管理コマンド

9.9.1 Showコマンド

9.9.1.1 show users

このコマンドにより設定ユーザ名およびその設定内容を表示します。このコマンドは読み書き権限のあるユーザにのみ使用することができます。システム上でSNMPが使用可能な場合にのみSNMPv3フィールドが表示されます。

Syntax
show users

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

User Name/ユーザー名: シリアルポート、Telnet、Webにログインするユーザ名。 空白エントリに名前を入力してIBPに新たなユーザーを追加できる。 ユーザ名には、最大8文字を使用することができます。大文字と小文字は区別されません。 Adminとguest2人のユーザーが工場側デフォルト値として含まれている。.

User Access Mode /ユーザーアクセス・モード : オペレータがIBP上のパラメータを変更できる (読み書き可) か、または閲覧のみ可能 (読み取り専用) かを示します。デフォルト設定では、管理者に読み書き可のアクセス、ゲストに読み取り専用のアクセスが与えられています。読み書き可は1ユーザ、読み取り専用は最大5ユーザまで設定可能です。

SNMPv3 Access Mode / SNMPv3アクセス・モード -: SNMPv3アクセスモードを示します。**Read- Write**に設定されている場合、SNMPv3ユーザはシステム上のパラメータを設定、検索することができます。**Read Only**に設定されている場合、SNMPv3ユーザはパラメータ情報の検索のみを行うことができます。SNMPv3アクセスモードは、CLIアクセスモードやWebアクセスモードとは異なります。

SNMPv3 Authentication: 特定のログインユーザに使用する認証プロトコルを示します。

SNMPv3 Encryption: 特定のログインユーザに使用する暗号化プロトコルを示します。

© 2010 富士通テクノロジー・ソリューションズ

9.9.1.2 show users authentication

このコマンドによりすべてのユーザおよび認証ログイン情報を表示します。また、デフォルトユーザに割り当てられた認証ログインリストも表示します。

Syntax
show users authentication

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

User/ユーザ ： 認証ログインリストが割り当てられたすべてのユーザを列記します。

System Login /システムログイン ： ユーザに割り当てられた、システムログインに使用する認証ログインリストを示します。

802.1x: ユーザに割り当てられた、802.1xポートセキュリティに使用する認証ログインリストを示します。

© 2010 富士通テクノロジー・ソリューションズ

9.9.2 設定コマンド

9.9.2.1 username

このコマンドにより空き領域がある場合に新規ユーザ (アカウント) を追加します。アカウントの<username>には最大8文字を入力することができます。名前にはハイフン (-) およびアンダーライン (_) を含めた英数字を使用することができます。<username>は大文字と小文字では区別されません。

6つのユーザ名を定義することができます。

このコマンドにより既存オペレータのパスワードを変更します。ユーザのパスワードは8文字以内です。ユーザ認証が許可された場合、または暗号化が有効である場合、パスワードは8文字の英数字にする必要があります。ユーザ名とパスワードは大文字と小文字では区別されません。パスワードを変更した場合、オペレータの前回のパスワードが要求されます。前回のパスワードがない場合はenterキーを押します。

Syntax
username <username> {password <0|7> <password> | nopassword} no username <username>

<username> -新規ユーザ名 (範囲：最大8文字)

no - 前回作成したユーザ名を削除します。

注 ： 管理ユーザのアカウントを削除することはできません。

nopassword - このコマンドにより既存オペレータのパスワードを空白に設定します。パスワードを変更した場合、オペレータの前回のパスワードが要求されます。前回のパスワードがない場合はEnterキーを押します

初期設定

No password

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.9.2.2 username snmpv3 authentication

このコマンドにより特定のログインユーザに使用する認証プロトコルを指定します。有効な認証プロトコルはnone、md5、shaです。md5またはshaを指定した場合、ユーザのログインパスワードはsnmpv3認証パスワードとして使用されます。<username>は、指定した認証プロトコルが使用されるログインユーザ名です。

Syntax
username snmpv3 authentication <username> {none | md5 | sha} no username snmpv3 authentication <username>

<username> - ログインユーザ名.

md5 - md5による認証方法

sha - shaによる認証方法

none - 認証方法なし

no - このコマンドにより特定のログインユーザに使用する認証プロトコルをnoneに設定します。<username>は、指定した認証プロトコルが使用されるログインユーザ名です。

初期設定

No authentication

コマンド・モード

グローバル・コンフィグ

9.9.2.3 username snmpv3 encryption

このコマンドにより特定のログインユーザに使用する暗号化プロトコルおよびキーを指定します。有効な暗号化プロトコルはnoneまたはdesです。desプロトコルには、コマンド行で指定するkeyが必要となります。Keyは最大16文字となります。desプロトコルを指定したがキーを与えていない場合、キーを入力するよう要求されます。noneを指定した場合、キーを与える必要はありません。<username>は、指定した暗号化プロトコルが使用されるログインユーザ名です。

Syntax
username snmpv3 encryption <username> {none | des <0|7> <key>} no username snmpv3 encryption <username>

<username> - ログインユーザ名.

des - des暗号化プロトコル

none - 暗号化プロトコルなし

no - このコマンドにより暗号化プロトコルをnoneに設定します。 <username>は、指定した暗号化プロトコルが使用されるログインユーザ名です。

初期設定

No encryption

コマンド・モード

グローバル・コンフィグ

9.9.2.4 username defaultlogin

このコマンドにより未設定ユーザがシステムにログインを行う際、認証ログインリストをそのユーザに割り当てます。設定内容は、ユーザがローカルで設定された場合、特定ユーザに割り当てられた認証ログインリストで上書きされます。この値が設定されていない場合、ユーザはローカル認証のみで認証されます。

Syntax
username defaultlogin <listname>

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.9.2.5 username login

このコマンドによりシステムログインに使用する特定の認証ログインリストを特定ユーザに割り当てます。<username>は設定済みの<username>、および<listname>は設定済みのログインリストである必要があります。

リモート認証が必要なログインリストがユーザに割り当てられた場合、認証が完了するまで、CLI、Web、telnetセッションからのインターフェイスへのアクセスはすべてブロックされます。

注記：IBPによる不測のロックアウトを防止するため、adminユーザに関連付けられたログインリストは変更できないようになっています。

Syntax
username login <user> <listname>

<user> - ログインユーザ名.

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.10 アップリンクセットコマンド

9.10.1 Showコマンド

このコマンドによりアップリンクセット情報を表示します。

Syntax
show uplink-set [<uplinkSetName>]

<uplinkSetName> -表示するアップリンクセット名

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Uplink Set Name / アップリンク・セット名 : アップリンクセット名を示します。

Logical Interface/論理インターフェイス: Active PortsおよびBackup Ports用のPplink Setの論理インターフェイス

External Ports /外部ポート :: アップリンクセットのメンバー。 メンバーは外部ポートである必要があります。

External Active Ports/アクティブな外部ポート: アクティブな外部ポート・メンバーをリストする。

External Backup Ports/外部バックアップ・ポート - 外部バックアップ・ポートをリストする。

Link State/リンク・ステート: アップリンクセットのリンクステートのステータス

Port Backup/ポート・バックアップ: アップリンクセットのポートバックアップのステータス

IGMP Snooping/IGMPスヌーピング: アップリンクセットのIGMPスヌーピングのステータス

LACP: アップリンクセットのLACPのステータス

9.10.2 設定コマンド

このコマンドによりアップリンクセットの作成または削除を行います。

Syntax
uplink-set <uplinkSetName> no uplink-set <uplinkSetName>

<uplinkSetName> -便宜のためアップリンクセットに関連付ける文字列。最大32文字の英数字を入力します。空欄にはできません。

no - このコマンドで既存のアップリンクセットを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりアップリンクセットへ（から）ポートを追加または削除します。

Syntax
uplink-set <uplinkSetName> no uplink-set <uplinkSetName>

<uplinkSetName> - 便宜のためアップリンクセットに関連付ける文字列。最大32文字の英数字を入力します。空欄にはできません。.

no - このコマンドによりアップリンクセットからポートを削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.11 ポートグループコマンド

9.11.1 Showコマンド

このコマンドによりポートグループ情報を表示します。

Syntax
show port-group [<portGroupName>]

<portGroupName> - 表示するポートグループ名

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Port Group Name/ポート・グループ名: ポートグループ名

Internal Ports/内部ポート: 内部ポートメンバーのリスト

Uplink Set Name/アップリンク・セット名 : アップリンク・セット名。

External Ports /外部ポート : ポートグループの外部ポートのリスト

9.11.2 設定コマンド

このコマンドによりポートグループの作成または削除を行います。

Syntax
port-group <portGroupName> [<uplinkSetName>] no port-group <portGroupName>

<uplinkSetName> -便宜のためアップリンクセットに関連付ける文字列。既存のアップリンクセットである必要があります。

<portGroupName> -便宜のためポートグループに関連付ける文字列。最大32文字の英数字を入力します。空欄にはできません。

no - このコマンドで既存のポートグループを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりポートグループへ (から) ポートを追加または削除します。

Syntax
port-group <portGroupName> no port-group <portGroupName>

<portGroupName> - 便宜のためポートグループに関連付ける文字列。. 既存のポートグループである必要があります。

no - このコマンドによりポートグループからポートを削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.12 VLANポートグループコマンド

9.12.1 Showコマンド

このコマンドによりVLANグループ情報を表示します。

Syntax
show vlan-group [<vlanGroupName>]

<vlanGroupName> -表示するVLANグループ名

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

VLAN Port Group Name/VLANポート・グループ名: VLANグループ名

VLAN ID: VLANグループのVLAN識別子。VLAN IDの範囲は1～4094

Internal Ports/内部ポート :内部インターフェイス。VLANグループのメンバー

Uplink Set Name/アップリンク・セット名 - 外部接続を行うための指定アップリンクセット

External Ports/ 外部ポート : 指定されたアップリンク・セットのメンバーである外部インターフェイス。

Native VLAN / ネイティブVLAN: ネイティブVLAN機能がこのVLANグループで対応しているかを示します。

© 2010 富士通テクノロジー・ソリューションズ

9.12.2 設定コマンド

このコマンドによりVLANグループを作成または破棄します。

Syntax
vlan-group <vlanGroupName> <1-4094> <uplinkSetName> no vlan-group <vlanGroupName>

<vlanGroupName> -便宜のためVLANグループに関連付ける文字列

<1-4094> - VLAN ID

<uplinkSetName> - VLANグループで外部接続となるアップリンクセット

no - このコマンドにより外部VLANグループのリンクステートを無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりVLANグループへ（から）ポートを追加または削除します。

Syntax
vlan-group <vlanGroupName> no vlan-group <vlanGroupName>

<vlanGroupName> - 便宜のためVLANグループに関連付ける文字列

no - このコマンドにより指定VLANグループからポートを削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

このコマンドにより特定VLANグループのネイティブVLANオプションを設定します。

Syntax
vlan-group-nativeVLAN <vlanGroupName> no vlan-group-nativeVLAN <vlanGroupName>

<vlanGroupName> -便宜のためVLANグループに関連付ける文字列

no - このコマンドによりネイティブVLANオプションをデフォルト値に設定します。

初期設定

無効

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.13 サービスLANコマンド

9.13.1 Showコマンド

このコマンドによりサービスLAN情報を表示します。

Syntax
show svc-lan [<svcLanName>]

<svcLanName> - 表示するサービスLAN名

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Service LAN Name/サービスLAN名: サービスLAN名

VLAN ID: サービスLANのVLAN ID

Internal Ports/内部ポート: サービスLANのメンバーである内部インターフェイス。

Uplink Set Name/アップリンク・セット名 : 外部接続を行うための指定アップリンクセット

External Ports /外部ポート: 指定されたアップリンク・セットのメンバーである外部インターフェイス。

9.13.2 設定コマンド

このコマンドによりサービスLANの作成または破棄を行います。

Syntax
svc-lan <svcLanName> <1-4094> <uplinkSetName> no svc-lan <svcLanName>

<svcLanName> -便宜のためサービスLANに関連付ける文字列

<1-4094> - VLAN ID

<uplinkSetName> - このサービスVLANで外部接続となるアップリンクセット

no - このコマンドにより指定サービスLANを破棄します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりサービスLANへ (から) ポートを追加または削除します。

Syntax
svc-lan <svcLanName> no svc-lan <svcLanName>

<svcLanName> -便宜のためサービスLANに関連付ける文字列

no - このコマンドにより特定サービスLANからポートを削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.14 サービスVLANコマンド

9.14.1 Showコマンド

このコマンドによりサービスVLAN情報を表示します。

Syntax
show svc-vlan [<svcVlanName>]

<svcVlanName> -表示するサービスVLAN名

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Service VLAN Name / サービスVLAN名 : サービスVLAN名

VLAN ID: サービスVLANのVLAN識別子。VLAN IDの範囲は1～4094

Internal Ports/内部ポート: サービスVLANのメンバーである内部インターフェイス。

Uplink Set Name/アップリンク・セット名 : 外部接続を行うための指定アップリンクセット

External Ports /外部ポート: 指定されたアップリンク・セットのメンバーである外部インターフェイス。

© 2010 富士通テクノロジー・ソリューションズ

9.14.2 設定コマンド

このコマンドによりサービスVLANを作成または破棄します。

Syntax
svc-vlan <svcVlanName> <1-4094> <uplinkSetName> no svc-vlan <svcVlanName>

<svcVlanName> -便宜のためサービスVLANに関連付ける文字列。

<1-4094> - VLAN ID

<uplinkSetName> - このサービスVLANで外部接続となるアップリンクセット。

no - このコマンドにより既存のサービスVLANを破棄します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりサービスVLANへ（から）ポートを追加または削除します。

Syntax
svc-vlan <svcVlanName> no svc-vlan <svcVlanName>

<svcVlanName> - 便宜のためサービスVLANに関連付ける文字列

no - このコマンドにより指定サービスVLANからポートを削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.15 分離コマンド

9.15.1 設定コマンド

このコマンドによりインターフェイスの分離モードを有効化または無効化します。通常、同じポートグループ内のすべてのインターフェイス間で通信が行われます。このポートグループの他のメンバーに対しインターフェイスを非表示設定し、そのインターフェイス上で受信したパケットをこのポートグループの他のメンバーではなく、アップリンクポートに転送させることができます。

Syntax
isolation no isolation

no –このコマンドによりこのインターフェイスの分離モードを無効化します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.16 ロックコマンド

9.16.1 lock

このコマンドによりIBPへのhttpアクセスをロックし、送信された「lock_identifier」にこのロックを付与し登録します。ロックを設定すると、「他のアプリケーションで管理されているため現在このIBPへアクセスできません。noを使用し、デフォルト値に戻してください」というメッセージがWeb-GUI上に表示されます。

Syntax
lock <lock_identifier> [EXCLUSIVE] no lock {<lock_identifier>|ALL}

< lock_identifier > -英数字の文字列（範囲：1～32文字）

no - このコマンドによりデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.16.2 lock_message

このコマンドによりロックを設定した際にIBPのWeb-GUI上に「HTMLの文字列を指定できるようにする必要があります。「lock_message default」を使用し、デフォルト値に戻してください」というメッセージを表示します。

Syntax
lock_message {<message_string>| default}

< message_string > -指定HTML文字列（範囲：1～512文字）

lock_message default - このコマンドによりデフォルト値に戻します。

初期設定

< message_string > : 「このインテリジェントブレードパネルは現在仮想IOマネージャに管理されているため、HTTPユーザインターフェイスでこのモジュールを設定することはできません。ロックを解除するには、ブレードサーバが仮想IOマネージャに管理されていない状態にする必要があります。仮想IOマネージャを使用せずにロックを解除するには、登録されている各ロック識別子に「no lock <lock_identifier>」コマンドを発行してください。」

コマンド・モード

グローバル・コンフィグ

9.16.3 lock_reset

このコマンドによりIBPを非ロック状態に戻し、すべてのロックを解除します。

Syntax
lock_reset

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.16.4 show lock

このコマンドによりロックステータスの情報、および登録されているロック識別子のリストを表示します。現在のロックメッセージが表示されます。

Syntax
show lock

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Lock Status: 現在のロックステータス

Lock Message: ロック設定時、IBPのWeb-GUI上に表示されるメッセージ

Identifier / 識別子 : このロックで登録された「lock_identifier」

State /ステート: None、Normal、またはExclusiveの値

9.17　ポートバックアップ

ポート·グループが生成されると2個のリンク·アグリゲーション·グループがそのポート·グループに関連付けられる。 2個のリンク·アグリゲーション·グループは内部でアクティブなバックアップ·ポートとして定義される。 2個のリンク·アグリゲーション·グループのうち1個は同時にアクティブ化される。 たとえば、アクティブなリンク·アグリゲーション·グループがリンク·アップであると、バックアップ·アグリゲーション·グループは遮断される(トラフィックの送受信は起こらない) 。 その他の場合、アクティブなアグリゲーション·グループがリンクダウンであれば (アクティブなアグリゲーション·グループの全メンバーがリンクダウン)、バックアップ·アグリゲーション·グループはアクティブ化される。 アクティブ集約グループがリンクアップに戻ると、バックアップ集約グループはアクティブでなくなる。

9.17.1　Showコマンド

このコマンドによりポートバックアップ情報を表示します。

Syntax
show port-backup [<uplinkSetName> [status] | status]

<uplinkSetName> - 表示するアップリンクセット名

初期設定

なし

コマンド·モード

特権 EXEC

表示メッセージ

Uplink Set Name/アップリンク·セット名: アップリンクセット名を示します。

Port Backup/ポート·バックアップ: ポートバックアップが有効であるか無効であるかを示します。

External Active Ports/アクティブな外部ポート: アクティブポートリストにあるポートを示します。

External Backup Ports/外部バックアップ·ポート: バックアップポートリストにあるポートを示します。

9.17.2　設定コマンド

このコマンドによりアップリンクセットのポートバックアップを有効化または無効化します。

© 2010 富士通テクノロジー·ソリューションズ

Syntax
port-backup <uplinkSetName> no port-backup <uplinkSetName>

<uplinkSetName> - 便宜のためアップリンクセットに関連付ける文字列。既存のアップリンクセットである必要があります。

no - このコマンドにより既存のポートグループのポートバックアップを無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりアップリンクセットのポートバックアップのフェールバック時間を設定します。

Syntax
port-backup <uplinkSetName> failback-time <value> no port-backup <uplinkSetName> failback-time

<uplinkSetName> - 便宜のためアップリンクセットに関連付ける文字列。既存のアップリンクセットである必要があります。

<value> - 時間の範囲は1～60秒。デフォルト値は60秒

no - 特定アップリンクセットのフェールバック時間をデフォルト値に設定します。

初期設定

60

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

このコマンドによりアクティブポートリストからバックアップポートリストへポートを移動します。

Syntax
port-backup no port-backup

no - このコマンドによりアクティブポートリストへポートを移動します。

制限：アクティブポートの最終メンバーをバックアップポートへ移動することはできません。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.18 リンクステートコマンド

この機能で、すべてのアップリンクポートが非アクティブの場合に、接続ブレードによりサーバブレードポートを無効にすることができます。切り替え時間を変更し、サーバブレードの重複LANポートの「高速」フェールオーバーを行うことができます。

9.18.1 Showコマンド

このコマンドによりリンクステート情報を表示します。

Syntax
show linkstate [<uplinkSetName>]

<uplinkSetName> - 表示するアップリンクセット名

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Uplink Set Name/アップリンク・セット名: アップリンクセットの名前

Linkstate /リンク・ステート:. このアップリンクセットのリンクステートが有効であるか無効であるかを示します。

9.18.2 設定コマンド

このコマンドによりアップリンクセットのリンクステートを有効化または無効化します。

Syntax
linkstate <uplinkSetName> no linkstate <uplinkSetName>

<uplinkSetName> - 便宜のためアップリンクセットに関連付ける文字列。既存のアップリンクセットである必要があります。

no - このコマンドにより既存のアップリンクセットのリンクステートを無効化します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.19 SNTPコマンド

9.19.1 Showコマンド

9.19.1.1 show sntp

このコマンドによりSNTPクライアントの現在時刻および設定内容を表示し、ローカル時刻が正しく更新されているかを表示します。

Syntax
show sntp

初期設定

なし

コマンド・モード

ユーザ Exec, 特権 EXEC

表示メッセージ

Last Update Time /最後の更新時間: 最終時計更新時刻

Last Unicast Attempt Time: 最終転送クエリ時刻 (unicastモード)

Last Attempt Status /最後の 試行ステータス -: 最終SNTP要求 (unicastモード) または非要求メッセージ (broadcastモード) のステータス

Broadcast Count: 最終リブート以降SNTPクライアントが受信し処理した、非要求ブロードキャストメッセージの現在の数

Time Zone: 設定タイムゾーン

© 2010 富士通テクノロジー・ソリューションズ

9.19.1.2 show sntp client

このコマンドによりSNTPクライアント設定を表示します。

Syntax
show sntp client

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Client Supported Modes: 対応しているSNTPモード (Broadcast、Unicast、Multicast)

SNTP Version SNTP バージョン : クライアントが対応しているSNTPの最新バージョン

Port /ポート : SNTPクライアントポート

Client Mode: 設定されているSNTPクライアントモード

Unicast Poll Interval: 2の累乗によるSNTPクライアントの秒単位のポール間隔値

Poll Timeout (Seconds): SNTPクライアントの秒単位のポールタイムアウト値

Poll Retry: SNTPクライアントのポール再試行値

9.19.1.3 show sntp server

このコマンドにより設定SNTPサーバ、およびSNTPサーバの設定を表示します。

Syntax
show sntp server

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Server IP Address /サーバIP アドレス: 設定SNTPサーバのIPアドレス

Server Type: サーバのアドレスタイプ

Server Stratum: 最後に受信した有効パケットの、サーバの要求階層

Server Reference ID: 最後に受信した有効パケットの、サーバの参照時計識別子

Server Mode: SNTPサーバモード

Server Max Entries: 許可されるSNTPサーバの合計数

Server Current Entries: 設定SNTPの合計数

各設定サーバ:

IP address/IPアドレス: 設定SNTPサーバのIPアドレス

Address Type/アドレス・タイプ: 設定SNTPサーバのアドレスタイプ

Priority/プライオリティ: 設定サーバのIPプライオリティタイプ

Version / バージョン: サーバのSNTPバージョン番号。unicastモードでサーバのクエリに使用するプロトコルバージョン

Port /ポート: サーバのポート番号

Last Attempt Time: 特定サーバの最終サーバ試行時刻

Last Update Status: サーバの最終サーバ試行ステータス

Total Unicast Requests: サーバへの要求数

Failed Unicast Requests: サーバからの失敗要求数

© 2010 富士通テクノロジー・ソリューションズ

9.19.2 設定コマンド

9.19.2.1 sntp broadcast client poll-interval

このコマンドにより<poll-interval>の値が6～16となる場合に、2の累乗によるSNTPブロードキャストクライアントのポール間隔を秒単位で設定します。

Syntax
sntp broadcast client poll-interval <poll-interval> no sntp broadcast client poll-interval

<poll-interval> -範囲は6～16

no - このコマンドによりSNTPブロードキャストクライアントのポール間隔をデフォルト値に戻します。

初期設定

デフォルト値は6

コマンド・モード

グローバル・コンフィグ

9.19.2.2 sntp client mode

このコマンドによりシンプルネットワークタイムプロトコル (SNTP) のクライアントモードを有効化し、broadcast、multicast、unicastモードのいずれかに設定します。

Syntax
sntp client mode [broadcast	unicast	multicast] no sntp client mode

no - このコマンドによりシンプルネットワークタイムプロトコル (SNTP) のクライアントモードを無効化します。



SNTP IPv4のマルチキャストアドレスは224.0.1.1.です。

SNTP IPv6 のマルチキャストアドレスはff05::101.です。

IPv6アドレスはbroadcastモードに対応していません。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.19.2.3 sntp client port

このコマンドによりSNTPクライアントポートIDと、ポーリング間隔を秒単位で設定します。

Syntax
sntp client port <portid> no sntp client port

<portid> - SNTPクライアントポートID、1～65536

初期設定

デフォルトポートIDは123

コマンド・モード

グローバル・コンフィグ

9.19.2.4 sntp unicast client poll-interval

このコマンドによりSNTPユニキャストクライアントのポール間隔を秒単位で設定します。

Syntax
sntp unicast client poll-interval <poll-interval> no sntp unicast client poll-interval

<poll-interval> - ポーリング間隔。値が6～10の場合、2^(値) 秒となります。

no - このコマンドによりSNTPユニキャストクライアントのポール間隔をデフォルト値に戻します。

初期設定

デフォルト値は 6 である。

コマンド・モード

グローバル・コンフィグ

9.19.2.5 sntp unicast client poll-timeout

このコマンドによりSNTPユニキャストクライアントのポールタイムアウトを秒単位で設定します。

Syntax
sntp unicast client poll-timeout <poll-timeout> no sntp unicast client poll-timeout

< poll-timeout > - 秒単位のポーリングタイムアウト。範囲は1～30

no - このコマンドによりSNTPユニキャストクライアントのポールタイムアウトをデフォルト値に戻します。

初期設定

デフォルト値は 5である。

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.19.2.6 sntp unicast client poll-retry

このコマンドによりSNTPユニキャストクライアントのポール再試行を秒単位で設定します。

Syntax
sntp unicast client poll-retry <poll-retry> no sntp unicast client poll-retry

< poll-retry> -秒単位のポーリング再試行。範囲は0～10

no - このコマンドによりSNTPユニキャストクライアントのポール再試行をデフォルト値に戻します。

初期設定

デフォルト値は 1である。

コマンド・モード

グローバル・コンフィグ

9.19.2.7 sntp server

このコマンドによりサーバアドレスがIPアドレスまたはドメイン名、およびアドレスタイプがIPv4、IPv6、またはDNSとなる場合に、SNTPサーバ (最大3つ) を設定します。プライオリティの値を1～3、バージョンの値を1～4、ポートIDの値を1～65535に、任意で設定することができます。

Syntax
sntp server <ipaddress/ipv6address/domain-name> <addresstype> [<1-3> [<version> [<portid>]]] no sntp server remove <ipaddress/ipv6address/domain-name>

<ipaddress/ipv6address/domain-name> - SNTPサーバのIPアドレス。

<addresstype> - アドレスタイプはipv4、ipv6、dns。

<1-3> -範囲は1～3。

<version> -範囲は1～4。

<portid> - 範囲は1～65535。

no - SNTPサーバ・エントリを削除する。 更新された構成をIBPに設定する。 構成変更は直ちに反映される

初期設定

なし.

コマンド・モード

グローバル・コンフィグ

9.19.2.8 sntp clock timezone

このコマンドによりIBPの内部時計のタイムゾーンを設定します。

Syntax
sntp clock timezone <name> <0-12> <0-59> {before-utc | after-utc}

<name> - タイムゾーン名、通常は省略表記 (範囲：1～15文字)

<0-12> - UTC前後の時間数 (範囲：0～12時間)

<0-59> - UTC前後の分数 (範囲：0～59分)

before-utc - UTC (東側) 前のローカルタイムゾーンを設定します。

after-utc - UTC (西側) 後のローカルタイムゾーンを設定します。

初期設定

Taipei 08:00 After UTC

コマンド・モード

グローバル・コンフィグ

9.19.2.9 sntp multicast client poll-internal

このコマンドによりSNTPマルチキャストクライアントのポール間隔を秒単位で設定します。

Syntax
sntp multicast client poll-interval <poll-interval> no sntp multicast client poll-interval

<poll-interval> - ポーリング間隔。値の範囲が6～10の場合、2^(値) 秒となります。

no – このコマンドによりSNTPマルチキャストクライアントのポール間隔をデフォルト値に戻します。

初期設定

デフォルト値は 6である。

コマンド・モード

グローバル・コンフィグ

9.20 セキュリティコマンド

9.20.1 Showコマンド

9.20.1.1 show users authentication

このコマンドによりすべてのユーザおよび認証ログイン情報を表示します。また、デフォルトユーザに割り当てられた認証ログインリストも表示します。

Syntax
show users authentication

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

User/ユーザー: 認証ログインリストが割り当てられているすべてのユーザを列記します。

System Login: ユーザに割り当てられた、システムログインに使用する認証ログインリストを示します。

802.1x: ユーザに割り当てられた、802.1xポートセキュリティに使用する認証ログインリストを示します。

9.20.1.2 show authentication

このコマンドによりすべての認証ログインリストの順列認証メソッドを表示します。

Syntax
show authentication

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Authentication Login List: 認証ログインリスト名を示します。

Method 1 /方法1: 特定の認証ログインリストに1つめのメソッドがあれば表示します。

Method 2 /方法2: 特定の認証ログインリストに2つめのメソッドがあれば表示します。

Method 3 /方法3: 特定の認証ログインリストに3つめのメソッドがあれば表示します。

9.20.1.3 show authentication users

このコマンドにより特定の認証ログインリストに割り当てられているユーザの情報を表示します。未設定のユーザにログインが割り当てられている場合、ユーザ列にユーザdefaultを表示します。

Syntax
show authentication users <listname>

<listname> -認証ログインリスト名

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

User Name/ユーザー名 : 特定の認証ログインリストに割り当てられたユーザを表示します。

Component /コンポーネント: 認証ログインリストが割り当てられているコンポーネント (Userまたは802.1x) を表示します。

9.20.1.4 show dot1x

このコマンドによりdot1x Administrativeモードのステータスを表示します。

Syntax
show dot1x

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Administrative Mode/管理モード: IBPの認証制御が有効であるか無効であるかを示します。

9.20.1.5 show dot1x detail

このコマンドにより特定ポートのグローバルdot1x設定の概要およびdot1x設定の詳細を表示します。

Syntax
show dot1x detail <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド･モード

特権 EXEC

表示メッセージ

Port /ポート: 設定を表示するインターフェイス

Protocol Version/プロトコル･バージョン: このポートに関連するプロトコルバージョン。dot1x仕様の最初のバージョンに対応するため、値は 1 となります。

PAE Capabilities/PAE機能: このポートのポートアクセスエンティティ (PAE) の機能。値はAuthenticatorまたはSupplicant

Authenticator PAE State/認証コードPAEのステート: 認証者PAE状態マシンの現在の状態。値はInitialize、Disconnected、Connecting、Authenticating、Authenticated、Aborting、Held、ForceAuthorized、ForceUnauthorized

Backend Authentication State/バックエンド認証ステート: バックエンド認証状態マシンの現在の状態。値はRequest、Response、Success、Fail、Timeout、Idle、Initialize

Quiet Period/静止時間: サプリカントの取得を試行しない時間を定義するための、このポート上の認証者状態マシンで使用する時間。値は秒数で表示され、範囲は 0～65535 です。

Transmit Period/送信時間: サプリカントへEAPOL EAP Request/Identityフレームを送信するタイミングを決定するための、特定ポート上の認証者状態マシンで使用するタイマー。値は秒数で表示され、範囲は 1～65535 です。

Supplicant Timeout/認証請求者タイムアウト: サプリカントをタイムアウトにするための、このポート上の認証者状態マシンで使用するタイマー。値は秒数で表示され、範囲は 1～65535 です。

Server Timeout: 認証サーバをタイムアウトにするための、このポート上の認証者で使用するタイマー。値は秒数で表示され、範囲は 1～65535 です。

Maximum Requests/最大要求回数: サプリカントをタイムアウトにする前に、このポート上の認証者状態マシンがEAPOL EAP Request/Identityを再送する最大回数。値の範囲は 1～10

Reauthentication Period/再認証時間: サプリカントの再認証実施を決定するための、このポート上の認証者状態マシンで使用するタイマー。 値は秒数で表示され、範囲は 1～65535 です。

Reauthentication Enabled/再認証有効化: このポートで再認証が有効であるかを示します。値はTrueまたはFalse

Key Transmission Enabled/キー送信有効化: 特定ポートのサプリカントへキーを送信するかを示します。値はTrueまたはFalse

Control Direction/制御方向: 特定ポートまたは複数ポートの制御方向を示します。値はbothまたはin

9.20.1.6 show dot1x statistics

このコマンドにより特定ポートのグローバルdot1x設定の概要およびdot1x統計データを表示します。

Syntax
show dot1x statistics <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Port /ポート: 統計データを表示するインターフェイス

EAPOL Frames Received/受信されたEAPOLフレーム: この認証符号で受信した、いずれかのタイプの有効EAPOLフレームの数

EAPOL Frames Transmitted/送信されたEAPOLフレーム: この認証符号で送信した、いずれかのタイプのEAPOLフレームの数

EAPOL Start Frames Received/受信されたEAPOL開始フレーム: この認証符号で受信した、EAPOL開始フレームの数

EAPOL Logoff Frames Received/受信されたEAPOLログオフ・フレーム: この認証符号で受信した、EAPOLログオフフレームの数

Last EAPOL Frame Version/直前のEAPOLフレーム・バージョン: 最後に受信したEAPOLフレームのプロトコルバージョン番号

Last EAPOL Frame Source/直前のEAPOLフレーム・ソース: 最後に受信したEAPOLフレームのソースMACアドレス

EAPOL Response/Id Frames Received/受信されたEAPOL応答/IDフレーム: この認証符号で受信したEAP response/identityフレームの数

EAP Response Frames Received/受信されたEAP応答フレーム: この認証符号で受信した有効EAP responseフレームの数

EAP Request/Id Frames Transmitted/送信されたEAP応答/IDフレーム: この認証符号で送信したEAP request/identityフレームの数

EAP Request Frames Transmitted/送信されたEAP要求フレーム: この認証符号で送信したEAP requestフレーム (request/identityフレームより古いもの) の数

Invalid EAPOL Frames Received/受信された無効なEAPOLフレーム: フレームタイプが識別されていない認証符号で受信した、EAPOLフレームの数

EAP Length Error Frames Received/受信されたEAP長エラー・フレーム: フレームタイプが識別されていない認証符号で受信した、EAPOLフレームの数

© 2010 富士通テクノロジー・ソリューションズ

9.20.1.7 show dot1x summary

このコマンドにより特定ポートまたはすべてのポートの、グローバルdot1x設定の概要およびdot1x設定の概要を表示します。

Syntax
show dot1x summary {<slot/port> | all}

<slot/port> - 必要なインターフェイス番号である。

all - すべてのインターフェイス。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Interface: 設定を表示するインターフェイス。

Control Mode / 制御モード: このポートの設定制御モード。値はforce-unauthorized、force-authorized、Auto (オート)

Operating Control Mode/動作制御モード: このポートが動作する制御モード。値はauthorized、unauthorized

Reauthentication Enabled/再認証有効化: このポートで再認証が有効であるかを示します。

Port Status /ポートステータス: 特定ポートのサプリカントへキーを送信するかを示します。

9.20.1.8 show dot1x users

このコマンドによりローカルで設定されたユーザの802.1xポートセキュリティユーザ情報を表示します。

Syntax
show dot1x users <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

User: 特定ポートへのアクセス権をローカルで設定されたユーザ

9.20.1.9 show radius-servers

このコマンドにより設定したRADIUSサーバの項目を表示します。

Syntax
show radius-servers

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

IP Address/IPアドレス: 設定したRADIUSサーバのIPアドレス

Port/ポート: このサーバで使用しているポート

Type/種類: Primaryまたはsecondary

Secret Configured /シークレット構成: Yes / No

Message Authenticator/メッセージ認証コード: RADIUSサーバに設定された、メッセージ認証符号の属性

9.20.1.10 show radius

このコマンドによりIBPにおけるRADIUSのさまざまな設定項目を表示します。

Syntax
show radius

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Current Server Host Address : 現在、認証に使用している設定サーバ

Number of Configured Servers/構成されたサーバ数: 認証サーバの設定IPアドレス

Number of retransmits: 要求パケットが再送される最大回数の設定値

Timeout Duration /タイムアウト時間: 要求の再送を行う秒単位の設定タイムアウト値

RADIUS Accounting Mode: DisableまたはEnabled

RADIUS Dead Time: RADIUSサーバがダウンした場合の設定復帰時間

RADIUS Attribute 4 Mode: RADIUS NAS-IP属性を有効化または無効化します。

RADIUS Attribute 4 Value: RADIUS NAS-IP値

9.20.1.11 show radius accounting

このコマンドにより設定RADIUSアカウンティングモード、アカウンティングサーバ、設定アカウンティングサーバの統計データを表示します。

Syntax
show radius accounting [statistics <ipaddr|hostname>]

<ipaddr|hostname> - IPアドレスまたはホスト名

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

任意のトークン「statistics <ipaddr|hostname>」が含まれていない場合、アカウンティングモード、およびRADIUSアカウンティングサーバ詳細情報のみが表示されます。

RADIUS Accounting Mode: Enabledまたはdisabled

Host Address: RADIUSアカウンティングサーバの設定値

Port/ポート : RADIUSアカウンティングサーバで使用されているポート

Secret Configured /シークレット構成: YesまたはNo

任意のトークン「statistics <ipaddr|hostname>」が含まれている場合、設定RADIUSアカウンティングサーバの統計が表示されます。表示されるRADIUSアカウンティングサーバの統計データは以下のとおりです。

RADIUS Accounting Server Host Address: 設定RADIUSアカウンティングサーバのホストアドレス値

Round Trip Time: 最新のAccounting- Responseと、RADIUSアカウンティングサーバからのAccounting-Requestと一致するAccounting-Request間の、センチ秒単位の時間間隔

Requests: このアカウンティングサーバに送信された、RADIUS Accounting-Requestパケット数。ただし再送分は含まれません。

Retransmission: RADIUSアカウンティングサーバに再送された、RADIUS Accounting-Requestパケット数。

Responses: アカウンティングポート上で受信した、このサーバからのRADIUSパケット数。

Malformed Responses: このサーバから受信した、異常RADIUS Accounting-Responseパケット数。異常パケットには、無効な長さのパケットも含まれます。ただし、不正な認証符号および不明なタイプは、異常アカウンティング応答には含まれません。

Bad Authenticators: このアカウンティングサーバから受信した、無効な認証符号のあるRADIUS Accounting-Responseパケット数

Pending Requests: タイムアウトとなっていない、または応答を受信していない、このサーバへ送信されたRADIUS Accounting-Requestパケット数

© 2010 富士通テクノロジー・ソリューションズ

Timeouts: このサーバへのアカウンティングタイムアウト数

Unknown Types: アカウンティングポートのサーバから受信した、不明タイプのRADIUSパケット数

Packets Dropped: アカウンティングポートのサーバから受信し、なんらかの理由によりドロップされたRADIUSパケット数

9.20.1.12 show radius statistics

このコマンドによりRADIUSまたは設定サーバの統計データを表示します。設定RADIUSサーバの統計データを表示するには、指定したIPアドレスが前回設定したRADIUSサーバのIPアドレスと一致する必要があります。実行すると以下のフィールドが表示されます。

Syntax
show radius statistics <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Server Host Address: サーバのIPアドレスまたはホスト名

Round Trip Time /ラウンド・トリップ時間: 最新のAccess-Reply/ Access-Challengeと、RADIUS認証サーバからのAccounting-Requestと一致するAccounting-Request間の、100分の1秒単位の時間間隔

Access Requests: このサーバに送信されたRADIUS Access-Requestパケット数。ただし、再送分は含まれません。

Access Retransmission: このRADIUS認証サーバに再送された、RADIUS Access-Requestパケット数。

Access Accepts: このサーバから受信した、有効パケットと無効パケットを含むRADIUS Access-Acceptパケット数。

Access Rejects: このサーバから受信した、有効パケットと無効パケットを含むRADIUS Access-Rejectパケット数。

Access Challenges: このサーバから受信した、有効パケットと無効パケットを含むRADIUS Access-Challengeパケット数。

Malformed Access Responses: このサーバから受信した、異常RADIUS Access-Responseパケット数。異常パケットには、無効な長さのパケットも含まれます。ただし、不正な認証符号やシグネチャ属性、または不明なタイプは、異常アクセス応答には含まれません。

Bad Authenticators/不正認証コード: このサーバから受信した、無効な認証符号またはシグネチャ属性を含む、RADIUS Access-Responseパケット数。

Pending Requests/要求中: タイムアウトとなっていない、または応答を受信していない、このサーバへ送信されるRADIUS Access-Requestパケット数

Timeouts/タイムアウト回数: このサーバへの認証タイムアウト数

Unknown Types/不明なイプ:認証ポートのサーバから受信した、不明タイプのRADIUSパケット数

© 2010 富士通テクノロジー・ソリューションズ

Packets Dropped/破棄パケット: 認証ポートのサーバから受信し、なんらかの理由によりドロップされたRADIUSパケット数

9.20.1.13 show tacacs

このコマンドによりTACACSの設定情報を表示します。

Syntax
show tacacs

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Global Timeout: すべてのサーバのTACACSのグローバルタイムアウト値を示します。

IP Address/IP アドレス: TACACSサーバ

Port /ポート: TACACSのポートナンバー

Timeout (sec): TACACSサーバが応答を行わない間の、秒単位のタイムアウト値

Priority: サーバプライオリティ (0は最高プライオリティ)

9.20.1.14 show port-security

このコマンドによりシステム全体のポートセキュリティ設定を表示します。

Syntax
show port-security

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Port Security Administration Mode: システム全体のポートロックモード

このコマンドにより特定のインターフェイスまたはすべてのインターフェイスのポートセキュリティ設定を表示します。

Syntax
show port-security { <slot/port> | all }

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Intf: インターフェイス番号

Admin Mode/管理モード: インターフェイスのポートロックモード

Dynamic Limit: 動的に割り当てるMACアドレスの最大数

Static Limit: 静的に割り当てるMACアドレスの最大数

Violation Trap Mode: バイオレーショントラップが有効であるかを示します。

Violation Shutdown: バイオレーションシャットダウンが有効であるかを示します。

このコマンドにより動的にロックされた、ポートのMACアドレスを表示します。

Syntax
show port-security dynamic <slot/port>

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

MAC Address/MACアドレス: 動的にロックされたMACアドレス

このコマンドにより静的にロックされた、ポートのMACアドレスを表示します。

Syntax
show port-security static <slot/port>

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

MAC Address/MACアドレス: 静的にロックされたMACアドレス

このコマンドによりロックされたポート上で破棄された最終パケットのソースMACアドレスを表示します。

Syntax
show port-security violation <slot/port>

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

MAC address: ロックされたポート上で破棄されたパケットのMACアドレス

9.20.2 設定コマンド

9.20.2.1 authentication login

このコマンドにより認証ログインリストを作成します。<listname>には、大文字と小文字で区別されない最大15文字の英数字を入力します。IBPで、最大10個の認証ログインリストを設定することができます。リストを作成すると、認証メソッド local が最初のメソッドに設定されます。

任意のパラメータ method1、 method 2、 method 3 のすべてまたはいずれかを使用した場合、メソッドの順列リストが認証ログインリスト内に設定されます。認証ログインリストがない場合、新規の認証ログインリストが作成された後、認証ログインリストに認証メソッドが設定されます。認証ログインメソッドは最大3つです。メソッドの値は、local、radius、reject、tacacsです。

localは、ローカルで保存されたユーザIDおよびパスワードが認証に使用されること、radiusは、ユーザIDとパスワードがRADIUSサーバを使用して認証されること、rejectは、ユーザ認証を行わないこと、tacacsは、ユーザIDとパスワードがTACACSを使用して認証されることを示します。

ユーザ認証では、認証試行が成功または失敗するまでユーザログインで認証メソッドを順番に試行します。

注記：デフォルト設定が含まれているデフォルトログインリストの内容は変更できません。

Syntax
authentication login <listname> [<method1>] [<method2>] [<method3>] no authentication login <listname>

<listname> - 認証ログインリストを作成します (範囲：最大15文字)

<method1 - 3> - メソッド値は local、radius、reject、tacacs

no - このコマンドにより特定の認証ログインリストを削除します。以下いずれかの条件がtrueの場合、削除は失敗となります。

ログインリスト名が無効である、または既存の認証ログインリストと一致しない。

特定の認証ログインリストがいずれかのユーザ、あるいはいずれかのコンポーネントの非設定ユーザに割り当てられている。

ログインリストが、デフォルト設定の含まれたデフォルトログインリストであり、「config authentication login create」を使用して作成されていない。デフォルトログインリストの削除はできません。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.2.2 username defaultlogin

このコマンドによりシステムへのログイン試行に使用する認証ログインリストを、非設定ユーザに割り当てます。この設定は、ユーザがローカルで設定されている場合、特定ユーザに割り当てられた認証ログインリストで上書きされます。この値が設定されていない場合、ユーザはローカル認証のみで認証されます。

Syntax

```
username defaultlogin <listname>
```

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.2.3 username login

このコマンドによりシステムログインに使用する特定の認証ログインリストを特定のユーザに割り当てます。<username>は設定された<username>、<listname>は設定されたログインリストである必要があります。

リモート認証が必要なログインリストがユーザに割り当てられている場合、すべてのCLI、web、telnetからのインターフェイスへのアクセスはすべて、認証が完了するまでブロックされます。

注記：IBPによる不測のロックアウトを防止するため、「admin」ユーザに関連付けられたログインリストは変更できないようになっています。

Syntax

```
username login <user> <listname>
```

<user> - ログインユーザ名.

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.3 Dot1x設定コマンド

9.20.3.1 dot1x initialize

このコマンドにより特定ポートの初期化シーケンスを開始します。このコマンドは、特定ポートの制御モードが「Auto（オート）」の場合のみ有効化されます。制御モードが「Auto（オート）」でない場合、エラーが返されます。

© 2010 富士通テクノロジー・ソリューションズ

Syntax
dot1x initialize <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権 EXEC

9.20.3.2 dot1x default-login

このコマンドにより認証ログインリストを、802.1xポートセキュリティの非設定ユーザに割り当てます。この設定は、ユーザがローカルで設定されている場合、特定ユーザに割り当てられた認証ログインリストで上書きされます。この値が設定されていない場合、ユーザはローカル認証のみで認証されます。

Syntax
dot1x defaultl-login <listname>

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.3.3 dot1x login

このコマンドにより特定の認証ログインリストを、802.1xポートセキュリティの特定ユーザに割り当てます。<user>パラメータは設定済みユーザ、<listname>パラメータは設定済み認証ログインリストである必要があります。

Syntax
dot1x login <user> <listname>

© 2010 富士通テクノロジー・ソリューションズ

<user> - ログインユーザ名.

<listname> - 認証ログインリスト

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.3.4 dot1x system-auth-control

このコマンドによりIBPのdot1x認証対応を有効化します。デフォルトで認証対応は無効となっています。無効に設定されているとdot1x設定は保持され、変更することができますが、アクティブにすることはできません。

Syntax
dot1x system-auth-control no dot1x system-auth-control

no - このコマンドによりIBPのdot1x認証対応を無効化します。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

9.20.3.5 dot1x user

このコマンドにより特定ポートまたはすべてのポートへのアクセス権をもつユーザのリストに、特定ユーザを追加します。<username>パラメータは設定済みユーザである必要があります。

Syntax
dot1x user <user> {<slot/port> | all} no dot1x user <user> {<slot/port> | all}

<user> - ログインユーザ名.

<slot/port> - 必要なインターフェイス番号である。

all - すべてのインターフェイス。

no - このコマンドにより特定ポートまたはすべてのポートへのアクセス権をもつユーザのリストからそのユーザを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.3.6 dot1x port-control

このコマンドによりすべてのポートに使用する認証モードを設定します。制御モードは以下のいずれかとなります。

force unauthorized / 非認証強制: 認証者PAEで、制御ポートを無条件で非認証に設定します。

force authorized / 認証強制: 認証コード・ポート・アクセス・エンティティ (PAE)は制御されるポートを無条件に認証に設定する。

Auto (オート) : 認証コードPAEはポート・モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Syntax
dot1x port-control all {Auto (オート) | force-authorized | force-unauthorized} no dot1x port-control all

all - すべてのインターフェイス。

no - このコマンドによりすべてのポートで使用する認証モードを「Auto (オート)」に設定します。

初期設定

Auto (オート)

コマンド・モード

グローバル・コンフィグ

このコマンドにより使用する認証モードを特定ポートに設定します。

force unauthorized / 非認証強制: 認証者PAEで、制御ポートを無条件で非認証に設定します。

force authorized / 認証強制: 認証コード・ポート・アクセス・エンティティ (PAE)は制御されるポートを無条件に認証に設定する。

Auto (オート) : 認証コードPAEはポート・モードを認証請求者、認証コード、および認証サーバの間の認証交換結果を反映するうに設定する。

Syntax
dot1x port-control {Auto (オート) | force-authorized | force-unauthorized} no dot1x port-control

no - このコマンドにより特定ポートで使用する認証モードを「Auto (オート)」に設定します。

初期設定

Auto (オート)

コマンド・モード

インターフェイス・コンフィグ

9.20.3.7 dot1x max-req

このコマンドによりサプリカントをタイムアウトするまでにポート上の認証者状態マシンがEAPOL EAP Request/Identityフレームを送信する最大回数を設定します。<1-10>の値は1～10の範囲となります。

Syntax
dot1x max-req <1-10> no dot1x max-req

<1-10> -最大回数 (範囲:1～10)

no - このコマンドによりサプリカントをタイムアウトするまでにポート上の認証者状態マシンがEAPOL EAP Request/Identityフレームを送信する最大回数を、デフォルト値の2に設定します。

初期設定

2

コマンド・モード

インターフェイス・コンフィグ

9.20.3.8 dot1x re-authentication

このコマンドにより特定ポートのサプリカントの再認証を有効化します。

Syntax
dot1x re-authentication no dot1x re-authentication

no - このコマンドにより特定ポートのサプリカントの再認証を無効化します。

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

9.20.3.9 dot1x re-reauthenticate

このコマンドにより特定ポートの再認証シーケンスを開始します。このコマンドは、特定ポートの制御モードが「Auto (オート)」の場合のみ有効化されます。制御モードが「Auto (オート)」でない場合、エラーが返されます。

Syntax
dot1x re-authenticate <slot/port>

<slot/port> - 必要なインターフェイス番号である。

初期設定

なし

コマンド・モード

特権 EXEC

© 2010 富士通テクノロジー・ソリューションズ

9.20.3.10 dot1x timeout

このコマンドによりポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定します。使用しているトークンおよび送信された値 (秒単位) により、異なるタイムアウト設定可能パラメータが設定されます。以下のトークンに対応しています。

reauth-period: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、サプリカントの再認証を行うタイミングを決定します。reauth-periodの値は1～65535である必要があります。

quiet-period: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、サプリカントの取得を行わない時間を定義します。quiet-periodの値は1～65535である必要があります。

tx-period: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、サプリカントへEAPOL EAP Request/Identityフレームを送信するタイミングを決定します。quiet-periodの値は1 ~ 65535である必要があります。

supp-timeout: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、サプリカントをタイムアウトします。supp-timeoutの値は1～65535である必要があります。

server-timeout: ポートの認証者状態マシンで使用されているタイマーの値を秒単位で設定し、認証サーバをタイムアウトします。supp-timeoutの値は1 - 65535である必要があります。

Syntax
dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period} <seconds> no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}

<seconds> - 値の範囲は1～65535

no – このコマンドによりポートの認証者状態マシンで使用されている秒単位のタイマーの値を、デフォルト値に設定します。使用しているトークンに該当するデフォルト値が設定されます。

初期設定

reauth-period: 3600 秒

quiet-period: 60 秒

tx-period: 30 秒

supp-timeout: 30 秒

server-timeout: 30 秒

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.20.4 Radius設定コマンド

9.20.4.1 radius accounting mode

このコマンドによりRADIUSアカウンティング機能を有効化します。

Syntax
radius accounting mode no radius accounting mode

no - このコマンドによりRADIUSアカウンティング機能をデフォルト値に設定します。つまり、RADIUSアカウンティング機能が無効となります。

初期設定

Disabled

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.20.4.2 radius-server host

このコマンドによりRADIUS認証サーバおよびRADIUSアカウンティングサーバを設定します。

「auth」トークンを使用している場合、このコマンドによりRADIUS認証サーバへの接続に使用するIPアドレスを設定します。1つのRADIUSクライアントあたり最大3つのサーバを設定することができます。設定サーバが最大数になると、noコマンドを実行しサーバが1つ削除されるまで、このコマンドは失敗となります。任意の<port>パラメータを使用している場合、このコマンドにより設定RADIUSサーバへの接続に使用するUDPポート番号を設定します。UDPポート番号を設定するには、IPアドレスが、前回設定されたRADIUS認証サーバのIPアドレスと一致する必要があります。ポート番号の範囲は1～65535、デフォルト値は1812です。

「acct」トークンを使用している場合、このコマンドによりRADIUSアカウンティングサーバに使用するIPアドレスを設定します。アカウンティングサーバは1つのみ設定できます。アカウンティングサーバが現在設定されている場合、このコマンドが成功する前に、noコマンドを使用し設定からそのサーバを削除する必要があります。任意の<port>パラメータを使用している場合、このコマンドによりRADIUSアカウンティングサーバへの接続に使用するUDPポートを設定します。指定したIPアドレスは、前回設定されたアカウンティングサーバのIPアドレスと一致する必要があります。ポートがすでにアカウンティングサーバに設定されている場合、前回設定された値が新規ポートで置き換えられます。ポート値の範囲は1～65535、デフォルト値は1813です。

Syntax
radius-server host {acct | auth} <ipaddr|hostname> [port] no radius-server host {acct | auth} <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名。

[port] - ポート番号 (範囲：1～65535)

no - このコマンドにより設定RADIUS認証サーバまたはRADIUSアカウンティングサーバを削除します。「auth」トークンを使用している場合、前回設定されたRADIUS認証サーバが設定から削除されます。同様に、「acct」トークンを使用している場合、前回設定されたRADIUSアカウンティングサーバが設定から削除されます。<ipaddr|hostname>パラメータは、前回設定されたRADIUS認証サーバまたはRADIUSアカウンティングサーバのIPアドレスまたはホスト名と一致する必要があります。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.20.4.3 radius-sever key

このコマンドによりRADIUSクライアントと、RADIUS認証サーバまたはRADIUSアカウンティングサーバ間の共有キーを設定します。使用しているトークンが「auth」か「acct」であるかによって、共有キーがRADIUS認証サーバまたはRADIUSアカウンティングサーバに設定されます。与えられたIPアドレスは、前回設定したサーバのIPアドレスと一致する必要があります。このコマンドを実行すると、共有キーを入力するよう表示されます。共有キーは20文字以内の英数字となります。

Syntax
radius-server key {acct | auth} <ipaddr|hostname> <0|7> <key-value>

<ipaddr|hostname> - IPアドレスまたはホスト名

<0|7> - 0 はプレーンテキスト形式のキー、7は暗号化形式のキーを示します。

<key-value> -共有キー。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.4.4 radius-server retransmit

このコマンドによりRADIUSサーバから応答を受信しなかった場合に要求パケットを再送する最大回数を設定します。再試行の値は1～15の整数となります。

Syntax
radius-server retransmit <retries> no radius-server retransmit

<retries> -最大回数（範囲：1～15）

no - このコマンドによりRADIUSサーバから応答を受信しなかった場合に要求パケットを再送する最大回数を、デフォルト値の10に設定します。

初期設定

10

コマンド・モード

グローバル・コンフィグ

9.20.4.5 radius-server timeout

このコマンドにより応答を受信しなかった場合にRADIUSサーバに要求を再送した後のタイムアウト値を秒単位で設定します。タイムアウト値は1～30の整数となります。

Syntax
radius-server timeout <seconds> no radius-server timeout

<seconds> -最大タイムアウト（範囲：1～30）

no - このコマンドにより応答を受信しなかった場合にRADIUSサーバに要求を再送した後の秒単位のタイムアウト値を、デフォルト値の6に設定します。

初期設定

6

コマンド・モード

グローバル・コンフィグ

9.20.4.6 radius-server msgauth

このコマンドにより特定サーバのメッセージ認証符号属性を有効化します。

Syntax
radius-server msgauth <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.4.7 radius-server primary

このコマンドによりRADIUSクライアントにプライマリRADIUS認証サーバを設定します。プライマリサーバは、RADIUS要求の処理に使用するようデフォルトで設定されているものです。残りの設定サーバは、プライマリサーバにアクセスできない場合にのみ使用されます。最大3つのサーバを各クライアントに設定することができます。このうち1つのサーバのみをプライマリとして設定することができます。プライマリサーバがすでにこのコマンドの実行前に設定されている場合、このコマンドで使用されるIPアドレスで指定されたサーバが新規のプライマリサーバとなります。IPアドレスは、前回設定されたRADIUS認証サーバのIPアドレスと一致する必要があります。

Syntax
radius-server primary <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.5 TACACS+設定コマンド

9.20.5.1 tacacs host

このコマンドによりTACACSサーバを設定します。

このコマンドを実行すると、コマンドモードがTACACSモードに変更され、指定した値をホストに設定します。

Syntax
tacacs host <ipaddr|hostname> no tacacs host <ipaddr|hostname>

<ipaddr|hostname> - IPアドレスまたはホスト名

no - このコマンドにより設定したTACACSサーバを削除します。<ipaddr|hostname>パラメータは、前回設定したTACACSサーバのIPアドレスまたはホスト名と一致する必要があります。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

このコマンドによりTACACSサーバの設定認証および暗号化キーを設定します。

Syntax
key [<0/7> <key-value>]

このコマンドにパラメータがない場合、キーの値は削除され、グローバルキーが使用されます。

注記：共有キーは最大32文字です。

<0/7> - 0 はプレーンテキスト形式のキー、7は暗号化形式のキーを示します。.

<key-value> - TACACS認証および暗号化キー

初期設定

なし

コマンド・モード

TACACSモード

このコマンドによりTACACSサーバのサービスポートを設定します。

Syntax
port [<0-65535>]

このコマンドにパラメータがない場合、ポートの値がデフォルト値に戻ります。

<0-65535> - TACACSサービスポート（範囲：0～65535）

初期設定

49

コマンド・モード

TACACSモード

このコマンドによりTACACSサーバのプライオリティを設定します。

Syntax
Priority [<0-65535>]

このコマンドにパラメータがない場合、プライオリティの値がデフォルト値に戻ります。

<0-65535> - TACACSサービスのプライオリティ（範囲：0～65535）

初期設定

0

コマンド・モード

TACACSモード

© 2010 富士通テクノロジー・ソリューションズ

このコマンドによりTACACSの指定接続タイムアウト値を設定します。

Syntax
timeout [<seconds>]

このコマンドにパラメータがない場合、タイムアウト値は削除され、グローバルタイムアウトが使用されます。

<seconds> - TACACSの接続タイムアウト値 (範囲：1～30)

初期設定

なし

コマンド・モード

TACACSモード

9.20.5.2 tacacs key

このコマンドによりTACACSサーバのグローバル認証および暗号化キーを設定します。

Syntax
tacacs key <0/7> <key-value> no tacacs key

注記：共有キーは最大32文字です。

<0/7> - 0 はプレーンテキスト形式のキー、7は暗号化形式のキーを示します。.

<key-value> - TACACS認証および暗号化キー

no - このコマンドによりTACACSサーバ共有キーを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.20.5.3 tacacs timeout

このコマンドによりTACACSのグローバル接続タイムアウト値を設定します。

Syntax
tacacs timeout <seconds> no tacacs timeout

<seconds> - TACACSの接続タイムアウト値（範囲：1～30）。

no - このコマンドによりタイムアウト値をデフォルト値に戻します。

初期設定

5

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.20.6 ポートセキュリティ設定コマンド

9.20.6.1 port-security

このコマンドによりシステムレベル (グローバル・コンフィグ) またはポートレベル (Interface Config) のポートロックを有効化します。

Syntax
port-security no port-security

初期設定

なし

コマンド・モード

グローバル・コンフィグ、インターフェイス・コンフィグ

9.20.6.2 port-security max-dynamic

このコマンドにより動的にロックされたMACアドレスを特定ポートに許可する最大数を設定します。

Syntax
port-security max-dynamic [<0-600>] no port-security max-dynamic

no - このコマンドにより動的にロックされたMACアドレスを特定ポートに許可する最大数をデフォルト値に戻します。

初期設定

600

コマンド・モード

インターフェイス・コンフィグ

9.20.6.3 port-security max-static

このコマンドにより静的にロックされたMACアドレスを特定ポートに許可する最大数を設定します。

Syntax
port-security max-static [<0-20>]

```
no port-security max-static
```

no - このコマンドにより静的にロックされたMACアドレスを特定ポートに許可する最大数をデフォルト値に戻します。

初期設定

20

コマンド・モード

インターフェイス・コンフィグ

9.20.6.4 port-security mac-address

このコマンドにより静的にロックされたMACアドレスのリストにMACアドレスを追加します。

Syntax

```
port-security mac-address <mac-addr> <1-4094>
no port-security mac-address <mac-addr> <1-4094>
```

<1-4094> - VLAN ID

<mac-addr> -静的MACアドレス

no - このコマンドにより静的にロックされたMACアドレスのリストからMACアドレスを削除します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.20.6.5 port-security mac-address move

このコマンドにより動的にロックされたMACアドレスを、静的にロックされたMACアドレスに変換します。

Syntax
port-security mac-address move

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ

9.20.6.6 port-security violation shutdown

このコマンドによりポートセキュリティのバイオレーションシャットダウン属性を有効化します。

Syntax
port-security violation shutdown no port-security violation shutdown

no - このコマンドによりポートセキュリティのバイオレーションシャットダウン属性を無効化します。

初期設定

Disabled

コマンド・モード

インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.20.7 LDAPコマンド

9.20.7.1 show ldap

このコマンドにより現在のLDAP設定を表示します。

Syntax
show ldap

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Server IP/サーバIP: LDAPサーバIP。デフォルト値は0.0.0.0

Server Port: LDAPサーバのTCPポート。デフォルト値は389

baseDN: ベース識別名。デフォルト値は空文字列

racName: バインドDNのRDN属性。デフォルト値は空文字列

racDomain: RDNを除いた部分バインドDN。デフォルト値は空文字列

9.20.7.2 ldap ip

このコマンドによりLDAPサーバIPを設定します。

Syntax
ldap ip <ipaddr> no ldap ip

<ipaddr> - IPアドレス 。

no - このコマンドによりIPアドレスをデフォルト値に戻します。

初期設定

0.0.0.0

コマンド・モード

グローバル・コンフィグ

9.20.7.3 ldap port

このコマンドによりLDAPサーバポートを設定します。

Syntax
ldap port <portid> no ldap port

<portid> - 1-65535

no - このコマンドによりLDAPサーバポートをデフォルト値に戻します。

初期設定

389

コマンド・モード

グローバル・コンフィグ

9.20.7.4 ldap baseDN

このコマンドによりbaseDNを設定します。

Syntax
ldap baseDN <baseDN> no ldap baseDN

<baseDN> -文字列

no - このコマンドによりbaseDNをデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.7.5 ldap racName

このコマンドによりracNameを設定します。

Syntax

```
ldap racName <racName>
no ldap racName
```

<racName> -文字列 。

no - このコマンドによりracNameをデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.20.7.6 ldap racDomain

このコマンドによりracDomainを設定します。

Syntax

```
ldap racDomain <racDomain>
no ldap racDomain
```

<racDomain> - string.

no - このコマンドによりracDomainをデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.21 差別化サービスコマンド

本章では、QOS差別化サービス (DiffServ) パッケージに使用するCLIコマンドについて説明します。

以下を指定し、複数段階でDiffServを設定します。

1. クラス
   - クラスを作成、削除する
   - クラスの一致基準を定義する

注 : 既存クラス定義から個別に一致基準を削除するには、そのクラスを削除し、再度作成します。

2. ポリシー
   - ポリシーを作成、削除する
   - クラスにポリシーを関連付ける
   - ポリシー／クラスの組み合わせのポリシー記述を定義する
3. サービス
   - 方向インターフェイス (インバウンドおよびアウトバウンド) へ (から) 、ポリシーを追加または削除する

パケットは、定義した基準によってフィルタ、処理されます。フィルタ基準はクラスにより、またその処理はポリシー属性により定義されます。ポリシー属性はクラスインターフェイスごとに定義され、基準が一致した場合に適用される属性となります。

パケット処理は、パケットの一致基準のテストで開始します。ポリシーは、ポリシー内でクラスが一致した場合にパケットに適用されます。

注記：all、any、aclのクラスタイプは、クラスを定義した際に指定される一致基準の妥当性に関係します。「any」のクラスタイプは順列シーケンスの一致基準を処理し、このクラスに指定した追加規則がリストに追加されます。「acl」のクラスタイプは、Diffservクラスが作成された際に各ACL規則定義を取り込み、規則リストを取得します。クラスタイプ「all」の一致基準を指定すると、除外しない一致基準フィールドの値が1つクラス定義で許可されるため、差異が発生します。フィールドがすでにクラスに指定されている場合、同じフィールドを指定するすべての後続試行が失敗となります。これには、別の形式による複数の方法でフィールドを指定する場合も含まれます。ただし、「exclude」オプションを指定した場合はこの制限が除外フィールドに適用されないため、これには含まれません。

クラス制限について：

- ネスト化クラスは以下のように制限されます。
- 「all」内は「all」
- 条件が「not」の場合、ネスト化されない
- クラスタイプが「acl」の場合、ネスト化されない
- 各クラスで 1 つの参照済みクラスをもつ
- 階層サービスポリシーはクラス定義で対応しない
- 一致したアクセスリストは参照のみ。クラスの基準となる

© 2010 富士通テクノロジー・ソリューションズ

- ACL規則は、クラス作成時にクラス一致基準としてコピーされる。クラスタイプは「any」
- 暗黙のACL規則「deny all」もコピーされる
- 「acl」のクラスタイプはネスト化されない

ネスト化クラスはクラス参照といい、別のクラスへの参照1つを特定のクラス定義に与え、それを他の一致基準と組み合わせることができます。参照済みクラスに追加を行うと、そのクラス定義を参照するすべてのクラスに影響を与えるため、参照済みクラスは参照でありコピーではありません。他のクラスから現在参照されているクラス定義への変更を行うと、すべての該当クラスの有効クラス定義となり、それ以外の場合、変更は拒否されます。クラス参照は、クラス定義から削除することができます。

クラス、ポリシー、サービスの概要および詳細情報を表示することができます。すべての設定情報はCLI、Web、SNMPのユーザインターフェイスからアクセスできます。

9.21.1 一般コマンド

プラットフォームの以下の項目を設定することができます。

9.21.1.1 diffserv

このコマンドによりDiffServ動作モードをアクティブに設定します。無効の場合、DiffServ設定を保持、変更することができますが、アクティブにすることはできません。有効の場合、DiffServサービスがアクティブとなります。

Syntax
diffserv

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.21.1.2 no diffserv

このコマンドによりDiffServ動作モードを非アクティブに設定します。無効の場合、DiffServ設定を保持、変更することができますが、アクティブにすることはできません。有効の場合、DiffServサービスがアクティブとなります。

Syntax
no diffserv

コマンド・モード

グローバル・コンフィグ

9.21.2 クラスコマンド

DiffServの「class」コマンドセットで以下を定義します。

- **Traffic Classification**で、DSCPに基づくBehavior Aggregate (BA) 、およびトラフィックのMulti- Field (MF) クラス (name、match criteria) を指定します。
- **Service Levels**で、BA転送クラス／サービスレベルを指定します。理論上、DiffServは1. Service/PHB、2. Traffic Classの2階層です。

このコマンドセットで、クラスの作成／削除、およびレイヤー3・レイヤー2・標準一致基準を指定するクラス一致コマンドによる一致を行います。クラス一致基準はクラス規則ともいい、1つまたは複数の規則からなるクラス定義ができないため、クラス全体を削除または再度作成する必要があります。

CLIコマンドルートはclass-mapです。

9.21.2.1 class-map

このコマンドによりtype match-all（全タイプに一致）、match-any（いずれかに一致）、match-access-group（アクセスグループに一致）の新規DiffServクラスを定義します。

Syntax
class-map [match-all] <class-map-name>

<class-map-name> はクラスを固有に識別する、大文字と小文字で区別される1～31文字の英数字です。

注 :クラス名「default」はリザーブされ、ここで使用することはできません。

一致基準を使用しない場合、このコマンドでクラスマップモードが入力されます。

<class-map-name>は既存のDiffServクラス名です。

注 :クラス名「default」はリザーブされ、ここでは許可されません。クラスタイプmatch-allは、すべての一致基準が、クラスのメンバーと判断されるパケットに対しtrueである必要があることを示します。クラスタイプmatch-access-groupは、各クラス一致基準がアクセスリスト（ACL）に基づき評価されることを示します。

<aclid>は、既存のACL番号を指定する整数です（有効なACL番号の範囲については、ACLのドキュメンテーションを参照）。matchaccess-groupのクラスタイプは、指定されたACL番号の現在の規則定義から、一致基準のセットをコピーします。単一のACL規則のすべてのエレメントはallのクラスタイプと同様、DiffServでグループ化セットと判断されます。anyのクラスについては、最低1つのクラス一致基準を、有効と判断されるクラスに指定する必要があります。

注 :クラス一致基準は参照済みアクセスリストat the time of class creationから取得されます。そのため、その後参照済みACL定義へ変更を行っても、DiffServクラスには影響を与えません。最新のACL定義を選択するには、DiffServクラスを削除、再度作成する必要があります。このコマンドは、既存のDiffServクラスにClass-Map コンフィグモードを入力するためのクラスタイプを指定せずに使用することができます。

注 :CLIモードは、コマンドが成功するとClass-Map コンフィグモードに変更されます。

コマンド・モード

グローバル・コンフィグ

9.21.2.2 no class-map

このコマンドにより既存のDiffServクラスを削除します。

Syntax
no class-map <class-map-name>

© 2010 富士通テクノロジー・ソリューションズ

<class-map-name> は既存のDiffServクラス名です。

注: クラス名「default」はリザーブされ、ここでは許可されません。このコマンドは問題となる場合があります。もし、1つ以上のポリシーまたは別のクラスでのを参照されると、削除に失敗します

コマンド・モード

グローバル・コンフィグ

9.21.2.3 class-map rename

このコマンドによりDiffServクラス名を変更します。

Syntax
class-map rename <class-map-name> <new-class-map-name>

<class-map-name> は既存のDiffServクラス名です。

<new-class-map-name>は、クラスを固有に識別する、大文字と小文字で区別される1～31文字の英数字による文字列です。

注: クラス名「default」はリザーブされ、ここで使用することはできません。

デフォルト

なし

コマンド・モード

グローバル・コンフィグ

9.21.2.4 match any

このコマンドによりすべてのパケットがそのクラスに属すると判断する一致基準を、特定のクラス定義に追加します。

Syntax
match any

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.5 match class-map

このコマンドにより他のクラスに定義された一致基準のセットを、特定のクラス定義に追加します。

Syntax
match class-map <refclassname>

<refclassname> は、一致基準が特定のクラス定義で参照される、既存のDiffServクラス名です。

注: この一致コマンドに[not]オプションはありません。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

制限： <classname>と<refclassname>のクラスタイプは同じである必要があります（つまりanyとany、またはallとall）。クラスタイプaclはこのコマンドで対応していません。<classname>と同じ名前の<refclassname>を指定することはできません（つまりクラス名の自己参照は許可されません）。1クラスで他のクラスを1つ参照することができます。<classname>から参照されている間、<refclassname>クラスの削除は失敗となります。

<classname>と<refclassname>を組み合わせた一致基準は、クラスタイプに基づき許可された組み合わせである必要があります。<refclassname>のクラス一致基準を後で変更する場合は、妥当性を維持する必要があり、そうでない場合変更は失敗となります。完全な参照クラスチェーン（predecessorクラスとsuccessorクラスの両方を含む）で作成されたクラス規則の合計数は、プラットフォーム指定の最大数を超えてはいけません。refclass規則の削除ごとに、クラス定義内の使用可能規則の最大数が1つずつ削除される場合もあります。

9.21.2.6 no match class-map

このコマンドにより他のクラスに定義された一致基準のセットを、特定のクラス定義から削除します。

Syntax
no match class-map <refclassname>

<refclassname> は、一致基準が特定のクラス定義で参照される、既存のDiffServクラス名です。

注: この一致コマンドに[not]オプションはありません。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.7 match dstip

このコマンドによりパケットの宛先IPアドレスに基づく一致基準を、特定のクラス定義に追加します。

Syntax
match dstip <ipaddr> <ipmask>

<ipaddr> IPアドレス

<ipmask> IPアドレスのビットマスク。注記：標準サブネットマスクと似ていますが、このビットマスクは連続させる必要はありません。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.8 match dstl4port

このコマンドによりキーワードや数値、あるいは数値範囲を使用したパケットの宛先レイヤー4ポートに基づく一致基準を、特定のクラス定義に追加します。

Syntax
match dstl4port {<portkey> | <0-65535>}

一致基準をキーワードとして指定するには、<portkey>の値に対応ポート名キーワードのうちの1つを使用します。現在対応している<portkey>の値はdomain、echo、ftp、ftpdata、http、smtp、snmp、telnet、tftp、wwwです。このそれぞれが同じポート番号に変換され、ポート範囲の開始および終了として使用されます。

数値で一致基準を指定するには、1つのレイヤー4ポート番号が必要となります。

ポート番号は0～65535の整数です。

数値範囲で一致基準を指定するには、2つのレイヤー4ポート番号で、連続するポート範囲を指定する必要があります。各ポート番号は0～65535の整数で、2つめの数は1つめの数と同じかそれ以上である必要があります。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.9 match ip dscp

このコマンドによりIPヘッダのService Typeオクテットの高位6ビット(低位2ビットはチェックされません)として定義された、パケット内のIP DiffServ Code Point(DSCP)フィールドの値に基づく一致基準を、特定のクラス定義に追加します。

Syntax
match ip dscp <value>

<dscpval>の値は、0～63の整数のいずれか、またはキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

注: ip dscp、ip precedence、ip tosの一致基準は、IPヘッダにある同じService Typeフィールドの一致基準を指定するための代替方法ですが、ユーザ表記は異なります。

注: すべてのDSCP値に一致基準を指定するには、<tosbits>を0、<tosmask>を03(16進数)に設定したmatch [not] ip tos <tosbits> <tosmask>コマンドを使用します。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.10 match ip precedence

このコマンドによりIPヘッダのService Typeオクテットの高位3ビット（低位5ビットはチェックされません）として定義された、パケット内のIP Precedenceフィールドの値に基づく一致基準を、特定のクラス定義に追加します。

Syntax
match ip precedence <0-7>

注: Ip dscp、ip precedence、ip tosの一致基準は、IPヘッダにある同じService Typeフィールドの一致基準を指定するための代替方法ですが、ユーザ表記はやや異なります。.

注: すべてのPrecedenceの値に一致基準を指定するには、<tosbits>を0、<tosmask>を1F（16進数）に設定したmatch [not] ip tos <tosbits> <tosmask>コマンドを使用します。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.11 match ip tos

このコマンドによりIPヘッダの全8ビットのService Typeオクテットとして定義された、パケット内のIP TOSフィールドの値に基づく一致基準を、特定のクラス定義に追加します。

Syntax
match ip tos <tosbits> <tosmask>

<tosbits>は00からffまでの2桁の16進数です。

<tosmask> は00からffまでの2桁の16進数です。

<tosmask>は、パケット内のIP TOSフィールドとの比較に使用する、<tosbits>内のビット位置を示します。例えば、ビット7が最大である場合にビット7と5が設定されビット1がクリアされているIP TOSの値を確認するには、<tosbits>にa0（16進数）、<tosmask>にa2（16進数）を使用します。

注: Ip dscp、ip precedence、ip tosの一致基準は、IPヘッダにある同じService Typeフィールドの一致基準を指定するための代替方法ですが、ユーザ表記はやや異なります。.

注: これはIP DSCP/Precedence/TOS一致基準の「フリーフォーム」バージョンであり、IP Service Typeフィールドのどのビットをチェックするかをユーザが指定することができます。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.12 match protocol

このコマンドによりキーワードまたは数値を使用したパケットのIP Protocolの値に基づく一致基準を、特定のクラス定義に追加します。

Syntax
match protocol {<protocol-name> | <0-255>}

<protocol-name> は、対応プロトコル名キーワードの1つです。現在対応している値はicmp、igmp、ip、tcp、udpです。注記：ipの値は、すべてのプロトコル番号に一致すると判断されます。数値を使用した一致基準を指定するには、プロトコル番号をIANAに割り当てられた標準値にし、0～255の整数として判断される必要があります。

注: このコマンドによりIANAに定義された現在のリストに対しプロトコル番号の値は検証しません。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.13 match srcip

このコマンドによりパケットのソースIPアドレスに基づく一致基準を、特定のクラス定義に追加します。

Syntax
match srcip <ipaddr> <ipmask>

<ipaddr> IPアドレス。

<ipmask> IPアドレスビットマスクを指定します。注記：標準サブネットマスクと似ていますが、このビットマスクは連続させる必要はありません。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.14 match srcl4port

このコマンドによりキーワードや数値、あるいは数値範囲を使用したパケットのソースレイヤー4ポートに基づく一致基準を、特定のクラス定義に追加します。

Syntax
match srcl4port {<portkey> | <0-65535>}

<portkey> は、対応するポート名キーワードの1つです（下記リスト参照）。

現在対応している<portkey>の値はdomain、echo、ftp、ftpdata、http、smtp、snmp、telnet、tftp、wwwです。

数値で一致基準を指定するには、1つのレイヤー4ポート番号が必要となります。ポート番号は0～65535の整数です。

数値範囲で一致基準を指定するには、2つのレイヤー4ポート番号で、連続するポート範囲を指定する必要があります。各ポート番号は0～65535の整数で、2つめの数は1つめの数と同じかそれ以上である必要があります。

デフォルト

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.15 match cos

このコマンドによりサービス値のクラス (単一タグ済みパケットのタグ、または二重VLANタグ済みパケットの第一タグあるいは外部802.1Qタグ) の一致基準を、特定のクラス定義に追加します。

Syntax
match cos <0-7>

初期設定

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.16 match destination-address mac

このコマンドによりパケットの宛先MACアドレスに基づく一致基準を、特定のクラス定義に追加します。<address> パラメータは、コロンで分割された2桁の16進数6組 (例：00:11:22:dd:ee:ff) の形式のレイヤー2 MACアドレスです。<mac-mask>パラメータは、コロンで分割された2桁の16進数6組 (例：ff:07:23:ff:fe:dc) の形式のレイヤー2 MACアドレスビットマスクで、連続する必要はありません。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match destination-address mac <address> <mac-mask>

<address> - レイヤー2 MACアドレスを指定します

<mac-mask> - レイヤー2 MACアドレスビットマスクを指定します。

初期設定

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.17 match ethertype

このコマンドによりethertypeの値に基づく一致基準を、特定のクラス定義に追加します。<ethertype>の値は**appletalk、arp、ibmsna、ipv4、ipv6、ipx、mplsmcast、mplsucast、netbios、novell、pppoe、rarp**のキーワード、または0x0600～0xFFFFの範囲のカスタムethertype値で指定します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match ethertype {<keyword> | <0x0600-0xFFFF>}

<keyword> - appletalk、arp、ibmsna、ipv4、ipv6、ipx、mplsmcastなどを指定します。

<0x0600-0xFFFF> - ethertype値を指定します。

初期設定

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.18 match secondary-cos

このコマンドによりサービス値のセカンダリクラス (二重VLANタグ済みパケットの内部802.1Qタグ) の一致基準を、特定のクラス定義に追加します。の一致基準を、特定のクラス定義に追加します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match secondary-cos <0-7>

初期設定

なし

コマンド・モード

Class-Map コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.21.2.19　match secondary-vlan

このコマンドによりレイヤー2セカンダリVLAN識別子フィールドの値（二重VLANタグ済みパケットの内部802.1Qタグ）に基づく一致基準を、特定のクラス定義に追加します。セカンダリVLAN IDは、0～4095の整数です。

注: このコマンドは、PG-SW112ハードウェアでは使用できません。

Syntax
match secondary-vlan <0-4095>

初期設定

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.20　match source-address mac

このコマンドによりパケットのソースMACアドレスに基づく一致基準を、特定のクラス定義に追加します。<address>パラメータは、コロンで分割された2桁の16進数6組（例：00:11:22:dd:ee:ff）の形式のレイヤー2 MACアドレスです。<mac-mask>パラメータは、コロンで分割された2桁の16進数6組（例：ff:07:23:ff:fe:dc）の形式のレイヤー2 MACアドレスビットマスクで、連続する必要はありません。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match source-address mac <address> <macmask>

<address> - レイヤー2 MACアドレスを指定します。

<macmask> - レイヤー2 MACアドレスビットマスクを指定します。

初期設定

なし

コマンド・モード

Class-Map コンフィグ

9.21.2.21 match vlan

このコマンドによりレイヤー2 VLAN識別子フィールドの値 (単一タグ済みパケットのタグ、またはVLANタグ済みパケットの第一タグまたは外部タグ) に基づく一致基準を、特定のクラス定義に追加します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
match vlan <0-4095>

初期設定

なし

コマンド・モード

Class-Map コンフィグ

9.21.3 ポリシーコマンド

DiffServの「policy」コマンドセットで、以下を定義します。

Traffic Conditioningで、トラフィッククラスに適用するトラフィック条件動作（ポリシング、marking、shaping）を指定します。

Service Provisioningで、サービスレベル（EF、AFなど）の帯域およびキュー深度管理要件を指定します。

ポリシーコマンドを使用し、クラスコマンドセットで定義されたトラフィッククラスと、1つまたは複数のQoSポリシー属性を関連付けます。関連付けは、サービスを作成するため特定方向のインターフェイスに割り当てられます。ポリシーが作成されたらポリシー名を指定します。

DiffServ CLIで、ユーザが1つのトラフィッククラスを1つのポリシーに関連付ける必要があるわけではありません。実際、複数のトラフィッククラスを1つのポリシーに関連付け、クラス定義に一致するパケットの特定処理を定義することができます。パケットが複数クラスの条件を満たした場合、クラスがポリシーに追加された順番に基づきプライオリティが決定するため、一番前にあるクラスが最優先されます。

このコマンドセットは、ポリシー作成／削除、クラス追加／削除、ポリシー属性で構成されています。注記：ポリシー内のクラスインスタンスからポリシー属性を削除するには、クラスインスタンスを削除してから再度ポリシーに追加します。既存のポリシー属性に関連付いている値は、クラスインスタンスを削除せずに変更することができます。

CLIコマンドルートはpolicy-mapです。

9.21.3.1 assign-queue

このコマンドにより関連トラフィックストリームが割り当てられているキューIDを修正します。queueidは0～n-1の整数で、nはデバイスが対応している送信キューの数です。

Syntax
assign-queue <0-7>

<0-7> - キューID。

(*)<0-6> - キューID。

*注: (*はスタッキングコマンドです。*

コマンド・モード

Policy-Class-Map コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.21.3.2 drop

このコマンドにより関連トラフィックストリームのすべてのパケットを受信時にドロップするよう指定します。

Syntax
drop

コマンド・モード

Policy-Class-Map コンフィグ

9.21.3.3 mirror

このコマンドにより関連トラフィックストリームのすべての受信パケットを、特定の送信インターフェイス (物理ポートまたはLAG) にコピーするよう指定します。

注: このコマンドは、Broadcom 5630xプラットフォームでは使用できません。

Syntax
mirror <slot/port>

<slot/port> - インターフェイス番号。

初期設定

なし

コマンド・モード

Policy-Class-Map コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.21.3.4 redirect

このコマンドにより関連トラフィックストリームのすべての受信パケットを、特定の送信インターフェイス (物理ポートまたはポートチャネル) にリダイレクトするよう指定します。

Syntax
redirect <slot/port>

コマンド・モード

Policy-Class-Map コンフィグ

9.21.3.5 conform-color

このコマンドによりカラートラフィックポリシングを有効化し、使用されている適合カラークラスマップを定義します。一致レベルのフィールド (simple、single-rate、two-rate policing) が指定されている場合、policeコマンドと共に使用します。<class-map-name>パラメータは、適合カラーおよび超過カラーで異なる名前を使用する必要がある場合、既存のDiffservクラスマップ名となります。

Syntax
conform-color <class-map-name>

<class-map-name> -適合カラーに異なる名前を使用する必要がある場合の、既存のDiffservクラスマップ名。

コマンド・モード

Policy-Class-Map コンフィグ

9.21.3.6 mark cos

このコマンドにより802.1pヘッダーの優先フィールド内にある、サービス値の特定クラスと関連付けられたトラフィックストリームの、すべてのパケットをマークします。パケットがこのヘッダーにない場合、1が挿入されます。CoSの値は0～7の整数です。

Syntax
mark cos <0-7>

<0-7> - CoS値の範囲は0～7。

コマンド・モード

Policy-Class-Map コンフィグ

Policy Type In//ポリシー・タイプ In

9.21.3.7 mark ip-dscp

このコマンドにより特定のIP DSCP値と関連付けられたトラフィックストリームの、すべてのパケットをマークします。

Syntax
mark ip-dscp <value>

<value>は、0～63の整数のいずれか、またはキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

コマンド・モード

Policy-Class-Map コンフィグ

Policy Type In/ポリシー・タイプ In

Incompatibilities Mark IP Precedence, Police （全形式）

© 2010 富士通テクノロジー・ソリューションズ

9.21.3.8 mark ip-precedence

このコマンドにより特定のIP Precedence値と関連付けられたトラフィックストリームの、すべてのパケットをマークします。IP Precedenceの値は0～7の整数です。

Syntax
mark ip-precedence <0-7>

コマンド・モード

Policy-Class-Map コンフィグ

Policy Type In/**ポリシー・タイプ** In

Incompatibilities Mark IP DSCP, Police （全形式）

9.21.3.9 police-simple

このコマンドにより特定クラスのトラフィックポリシングスタイルを確立します。

Syntax
police-simple {<1-4294967295> <1-128> conform-action {drop | set-cos-transmit <0-7> | set-prec-transmit <0-7> | set-dscp-transmit <value> | transmit} [violate-action {drop | set-prectransmit <0-7> | set-dscp-transmit <0-63> | transmit}]}

policeコマンドでは単一のデータレートとバーストサイズの形式を使用し、以下2通りの結果となります。

<conform-action & violate-action>：一致データレートがキロビット／秒（Kbps）単位で指定され、1～4294967295の整数となります。一致バーストサイズはキロバイト（KB）単位で指定され、1～128の整数となります。結果で実施される動作はdrop、set-dscp-transmit、set-prec-transmit、transmitです。policeコマンドの形式で、一致動作がtransmitに戻り、バイオレーション動作がdropに戻ります。動作はスタイルを設定するとこのコマンドで設定することができます。**<set-cos-transmit>**で、プライオリティの値が要求され、0～7の整数で指定されます。**<set-dscp-transmit>**が要求され、0～63の整数のいずれか、またはキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

<set-prec-transmit>で、IP Precedenceの値が要求され、0～7の整数で指定されます。

コマンド・モード

Policy-Class-Map コンフィグ

Restrictions/制限policeコマンドのsimpleのみが特定ポリシーのクラスインスタントに許可されます。

Policy Type In//**ポリシー・タイプ** In

Incompatibilities/非互換 Mark COS, Mark IP DSCP, Mark IP Precedence

© 2010 富士通テクノロジー・ソリューションズ

9.21.3.10 class

このコマンドにより後続ポリシー属性記述を使用しトラフィッククラスの処理を定義するため、特定ポリシー内にクラス定義のインスタンスを作成します。

Syntax
class <classname>

<classname> は既存のDiffServクラス名です。注記：このコマンドにより特定ポリシーがクラス定義への参照を作成します。

コマンド・モード

Policy-Class-Map コンフィグ

9.21.3.11 no class

このコマンドにより特定クラスのインスタンスおよび定義済み処理を、特定ポリシーから削除します。

Syntax
no class <classname>

<classname> は既存のDiffServクラス名です。注記：このコマンドにより特定ポリシーのクラス定義への参照を削除します。

コマンド・モード

Policy-Class-Map コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.21.3.12 policy-map

このコマンドにより新規のDiffServポリシーを確立します。<policyname>パラメータはポリシーを固有に識別するための、大文字と小文字で区別される1～31文字の英数字です。ポリシーのタイプはパラメータに示されているインバウンドトラフィックの方向となります。

Syntax
policy-map <policyname> [in] no policy-map <policyname>

コマンド・モード

グローバル・コンフィグ

Policy Type In//ポリシー・タイプ In

9.21.3.13 policy-map rename

このコマンドによりDiffServポリシー名を変更します。<policyname>は既存のDiffServクラス名です。<newpolicyname>パラメータはポリシーを固有に識別するための、大文字と小文字で区別される1～31文字の英数字です。

Syntax
policy-map rename <policyname> <newpolicyname>

<policyname> -旧ポリシー名。

<newpolicyname> -新規ポリシー名。

コマンド・モード

グローバル・コンフィグ

Policy Type In//ポリシー・タイプ In

9.21.4 サービスコマンド

DiffServの「service」コマンドセットで、以下を定義します。

Traffic Conditioning：DiffServトラフィック条件ポリシー（ポリシーコマンドで指定）を、受信方向のインターフェイスに割り当てます。

Service Provisioning：DiffServサービス提供ポリシー（ポリシーコマンドで指定）を、送信方向のインターフェイスに割り当てます。

サービスコマンドで、方向インターフェイスに定義済みポリシーを付与します。1ポリシーのみを、特定方向のインターフェイスにいつでも割り当てることができます。ポリシータイプ（in、out）は、付与するインターフェイスの方向と一致する必要があります。

このコマンドセットでサービスの追加／削除を行います。

CLIコマンドルートはservice-policyです。

9.21.4.1 service-policy

このコマンドにより特定方向のインターフェイスにポリシーを付与します。

Syntax
service-policy in <policy-map-name>

このコマンドをInterface Configモードで使用し、ポリシーを特定のインターフェイスに付与することができます。あるいは、このコマンドをGlobal Configモードで使用し、すべてのシステムインターフェイスにポリシーを付与することもできます。方向の値はinまたはoutです。

<policy-map-name>は既存のDiffServポリシー名であり、タイプがインターフェイスの方向と一致する必要があります。注記：このコマンドによりサービスによりポリシーに参照が作成されます。

注: このコマンドによりインターフェイス上のDiffServを有効化します（特定方向）。その他のDiffServ用インターフェイス管理の「mode」コマンドはありません。

注: このコマンドは、ポリシー定義内の属性がインターフェイスの上限を超えると失敗となります。ポリシーがインターフェイスに正しく付与されると、インターフェイス上限バイオレーションとするポリシー定義を変更してもそのポリシー変更は失敗となります。

コマンド・モード

グローバル・コンフィグ（すべてのシステムインターフェイス用）

インターフェイス・コンフィグ（特定のインターフェイス用）

Restrictions/制限　1ポリシーのみを、特定方向のインターフェイスにいつでも付与することができます。

© 2010 富士通テクノロジー・ソリューションズ

9.21.4.2 no service-policy

このコマンドにより特定方向のインターフェイスからポリシーを削除します。

Syntax
no service-policy in <policy-map-name>

このコマンドをInterface Configモードで使用し、ポリシーを特定のインターフェイスから削除することができます。あるいは、このコマンドをGlobal Configモードで使用し、現在ポリシーが付与されているすべてのシステムインターフェイスからポリシーを削除することもできます。方向の値はinまたはoutです。

<policy-map-name> は、既存のDiffServポリシー名です。注記：このコマンドによりサービスによりポリシーへの参照が削除されます。

注: このコマンドによりインターフェイス上のDiffServを無効化します（特定方向）。

その他のDiffServ用インターフェイス管理の「mode」コマンドはありません。

コマンド・モード

グローバル・コンフィグ（すべてのシステムインターフェイス用）

インターフェイス・コンフィグ（特定のインターフェイス用）

© 2010 富士通テクノロジー・ソリューションズ

9.21.5 Showコマンド

DiffServで「show」コマンドセットを使用し、以下の設定とステータス情報を表示します。

- クラス
- ポリシー
- サービス

この情報は、概要または詳細形式で表示することができます。ステータス情報は、DiffServ管理モードが有効の場合にのみ表示され、それ以外の場合は表示されません。また、「show」コマンドでDiffServの一般情報をいつでも表示することができます。

9.21.5.1 show diffserv

このコマンドによりメインDiffServプライベートMIBテーブルの現在数および最大数の列や現在の管理モード設定などの、DiffServ一般ステータスグループ情報を表示します。

Syntax
show diffserv

初期設定

なし

コマンド・モード

特権 Execおよびユーザ Exec

表示メッセージ

DiffServ Admin Mode/DiffServの管理モード: DiffServ管理モードの現在の値

Class Table Size Current/Max: クラステーブルのエントリ（列）の現在数または最大数

Class Rule Table Size Current/Max: クラス規則テーブルのエントリ（列）の現在数または最大数

Policy Table Size Current/Max: ポリシーテーブルのエントリ（列）の現在数または最大数

Policy Instance Table Size Current/Max: ポリシーインスタンステーブルのエントリ（列）の現在数または最大数

Policy Attribute Table Size Current/Max: ポリシー属性テーブルのエントリ（列）の現在数または最大数

Service Table Size Current/Max: サービステーブルのエントリ（列）の現在数または最大数

© 2010 富士通テクノロジー・ソリューションズ

9.21.5.2 show diffserv service

このコマンドにより特定のインターフェイスおよび方向のポリシーサービス情報を表示します。

Syntax
show diffserv service <slot/port> in

<slot/port>で、システムの有効スロット番号およびポート番号を指定します。directionパラメータは、インターフェイスの対象方向を示します。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

DiffServ Admin Mode: DiffServ管理モードの現在の設定。付与されたポリシーは、DiffServのモードが有効の場合にインターフェイス上で有効化されます。

Interface/インターフェイス: インターフェイスのスロット番号およびポート番号 (スロット／ポート)

Direction/方向: このインターフェイスサービスのトラフィック方向

Operational Status: DiffServサービスインターフェイスの現在の動作ステータス

Policy Name: 表示方向のインターフェイスに付与されたポリシー名

Policy Details: 付与されたポリシー詳細。内容はshowポリシーマップの<policymapname>コマンドと同じです (ここでの内容説明は省略します)。

9.21.5.3 show diffserv service brief

このコマンドによりDiffServポリシーが付与された、システム上のすべてのインターフェイスを表示します。directionパラメータは任意です。指定されている場合、その方向のサービスのみが表示されます。

Syntax
show diffserv service brief [in]

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

DiffServ Admin Mode/DiffServの管理モード: DiffServ管理モードの現在の設定。付与されたポリシーは、DiffServのモードが有効の間、インターフェイス上のみでアクティブとなります。

以下の情報はインターフェイスおよび方向について繰り返されます（付与されたポリシーで設定されたインターフェイスのみが表示されます）：

Interface/インターフェイス: インターフェイスのスロット番号およびポート番号（スロット／ポート）

Direction/方向: このインターフェイスサービスのトラフィック方向

Operational Status/動作状態: DiffServサービスインターフェイスの現在の動作ステータス

Policy Name/ポリシー名: 表示方向のインターフェイスに付与されたポリシー名

9.21.5.4 show class-map

このコマンドにより特定クラスのすべての設定情報を表示します。

Syntax
show class-map [<classname>]

<classname> は既存のDiffServクラス名です。

初期設定

なし

コマンド・モード

特権 Execおよびユーザ Exec

表示メッセージ

© 2010 富士通テクノロジー・ソリューションズ

Class Name: クラス名

Class Type:このクラスに対し一致基準が評価される方法を示すクラスタイプ（all、any、acl）。クラスタイプallは、このクラスに定義された一致基準が同時に評価され、すべてtrueの場合にクラスが一致していることを示します。タイプanyは、一致基準が順番に評価され、いずれか1つがtrueの場合にクラスが一致していることを示します。タイプaclは複合方法で評価するもので、各ACL規則によってグループ化と評価が同時に行われたものが順番に評価されます。

Match Criteria: Match Criteriaフィールドは、設定されているかどうかのみを示すもので、ユーザが入力した順番で内容が表示されます。クラスタイプに基づき評価が行われます。Match Criteriaフィールドの値は、Class of Service、Destination IP Address、Destination Layer 4 Port、Destination MAC Address、Every、IP DSCP、IP Precedence、IP TOS、Protocol Keyword、Reference Class、Source IP Address、Source Layer 4 Port、Source MAC Address、VLANです。

Values: Match Criteriaの値を示します。

Excluded: Match Criteriaが除外されているかを示します。クラス名が指定されていない場合、このコマンドですべての定義済みDiffServクラスの一覧を表示します。表示されるフィールドは以下のとおりです

Class Name: クラス名。

Class Type:このクラスに対し一致基準が評価される方法を示すクラスタイプ（all、any、acl）。クラスタイプallは、このクラスに定義された一致基準が同時に評価され、すべてtrueの場合にクラスが一致していることを示します。タイプanyは、一致基準が順番に評価され、いずれか1つがtrueの場合にクラスが一致していることを示します。タイプaclは複合方法で評価するもので、各ACL規則によってグループ化と評価が同時に行われたものが順番に評価されます。

ACL Number: クラス作成時にクラス一致基準を定義するためのACL番号。クラスタイプaclの場合のみこのフィールドを使用します（注記：ACLの内容は、クラス作成後変更されている場合があります）。

Ref Class Name: 特定のクラス定義で参照された一致基準である、既存のDiffServクラス名。

9.21.5.5 show policy-map

このコマンドにより特定ポリシーのすべての設定情報を表示します。

Syntax
show policy-map [<policy-map-name>]

<policy-map-name> は既存のDiffServポリシー名です。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Policy Name: ポリシー名

Policy Type: ポリシー定義がインバウンドであるかアウトバウンドであるかを示します。

以下の情報はこのポリシーに関連する各クラスについて繰り返されます：

（実際に設定されたポリシー属性のみが表示されます）：

Class Name: クラス名。

Mark CoS: アウトバウンドパケットの802.1pヘッダーで設定されたサービス値のクラスを示します。mark cosを指定していない場合は表示されません。

Mark IP DSCP: このクラスに一致するトラフィックのDSCPとして使用されるmark／re-markの値を示します。police-two-rateコマンドを使用してmark ipの記述が指定されていない場合、またはこのポリシーに従ったクラスにポリシングが使用されている場合は表示されません。

Mark IP Precedence: このクラスに一致するトラフィックのIP Precedenceとして使用されるmark／re-markの値を示します。このポリシーに従ったクラスに、mark DSCPまたはポリシングが使用されている場合は表示されません。

Policing Style: ポリシングのスタイルがあればsimpleと表示します。

Committed Rate (Kbps): シンプルポリシングのコミットレートをsingle-rate policingおよびtwo-rate policingで表示します。

Committed Burst Size (KB): シンプルポリシングのコミットバーストサイズを示します。

Conform Action: policingパラメータに適合すると判断されたパケットで適用されている現在の設定。このポリシーに従ったクラスでポリシングが使用されていない場合は表示されません。

Conform COS Value: 適合動作がmarkcosである場合、プライオリティマークの値を示します。

Conform DSCP Value: 適合動作がmarkdscpである場合、DSCPマークの値を示します。

Conform IP Precedence Value: 適合動作がmarkprecである場合、IP Precedenceマークの値を示します。

Non-Conform Action: policingパラメータに適合しない判断されたパケットで適用されている現在の設定。このポリシーに従ったクラスでポリシングが使用されていない場合は表示されません。

Non-Conform DSCP Value: 適合動作がmarkdscpである場合、DSCPマークの値を示します。

Non-Conform IP Precedence Value: 適合動作がmarkprecである場合、IP Precedenceマークの値を示します。

© 2010 富士通テクノロジー・ソリューションズ

Bandwidth: リザーブされた最低帯域をパーセントまたはキロビット／秒のいずれかで示します。

Policy Name: ポリシー名（注記：ポリシーの表示は作成順ではありません）

Policy Type: ポリシー定義がインバウンドであるかアウトバウンドであるかを示します。

Class Members: このポリシーに関連するすべてのクラス名の一覧を表示します。

9.21.5.6 show policy-map interface

このコマンドにより特定のインターフェイスおよび方向について、ポリシー関連の統計データを表示します。

Syntax
show policy-map interface <slot/port> in

<slot/port> で、システムの有効スロット番号およびポート番号を指定します。directionパラメータは、インターフェイスの対象方向を示します。

コマンド・モード

特権 EXEC

表示メッセージ

Interface/インターフェイス: インターフェイスのスロット番号およびポート番号（スロット／ポート）

Direction/方向: このインターフェイスサービスのトラフィック方向。inまたはout

Operational Status/動作状態 ：DiffServサービスインターフェイスの現在の動作ステータス

Policy Name/ポリシー名: 表示方向のインターフェイスに付与されたポリシー名

Interface Offered Octets/Packets: 定義済みのDiffServ処理が適用される前に、特定方向のサービスインターフェイスに与えられたオクテット／パケットの累積数

Interface Discarded Octets/Packets: DiffServ処理のため、特定方向のサービスインターフェイスにより破棄されたオクテット／パケットの累積数

Interface Sent Octets/Packets: 定義済みのDiffServ処理が適用された後に、特定方向のサービスインターフェイスから転送されたオクテット／パケットの累積数。この場合の転送とは、スイッチ機能やルーティング機能、またはアウトバウンドリンク送信エレメントなど、データパス内の次の機能エレメントにトラフィックストリームが送信されたことを示します。

以下の情報はこのポリシー内の各クラスインスタンスについて繰り返されます：

Class Name: クラスインスタンス名

In Offered Octets/Packets: 定義済みのDiffServ処理が適用される前に、このクラスインスタンスに与えられたオクテット／パケットの数。方向が「in」の場合のみ表示されます。

In Discarded Octets/Packets: トラフィッククラスのDiffServ処理のため、このクラスインスタンスで破棄されたオクテット／パケットの数。方向が「in」の場合のみ表示されます。

Tail Dropped Octets/Packets: 送信キューからのテールドロップ、特にトラフィックシェーピングにより破棄された、オクテット／パケットの数。プラットフォームによってはこの数に対応していない場合があります。方向が「out」の場合のみ表示されます。

Random Dropped Octets/Packets: WREDアクティブキュー深度管理のトラフィックシェーピングのため破棄された、オクテット／パケットの数。この数はすべてのプラットフォームで対応しているわけではなく、ポリシー属

性にランダムドロップが含まれたクラスインスタンスのみに使用されます。方向が「out」の場合のみ表示されます。

Shape Delayed Octets/Packets: トラフィックシェーピングのため遅延したオクテット／パケットの数。この数はすべてのプラットフォームで対応しているわけではなく、ポリシー属性にランダムドロップが含まれたクラスインスタンスのみに使用されます。方向が「out」の場合のみ表示されます。

Sent Octets/Packets: 定義済みのDiffServ処理が実施された後、このクラスインスタンスに転送されたオクテット／パケットの数。この場合の転送とは、スイッチ機能やルーティング機能、またはアウトバウンドリンク送信エレメントなど、データパス内の次の機能エレメントにトラフィックストリームが送信されたことを示します。方向が「out」の場合のみ表示されます。

注: 上記のカウンタはすべてのプラットフォームで対応しているわけではありません。対応しているカウンタのみが表示されます。

9.21.5.7 show service-policy

このコマンドにより特定方向のすべてのインターフェイスのポリシー関連統計データを表示します。Directionパラメータは、インターフェイスの対象方向を示します。このコマンドでルートリフレクタクライアントを有効化または無効化します。ルートリフレクタクライアントは、AS全体にルートを再度アドバタイズするルートリフレクタに従います。値はenableまたは*disable*です。

Syntax
show service-policy [in]

コマンド・モード

特権 EXEC

表示メッセージ

以下の情報は各インスタンスおよび方向について繰り返されます（付与されたポリシーに設定されたインターフェイスのみが表示されます）：

Interface: インターフェイスのスロット番号およびポート番号（スロット／ポート）

Operational Status: DiffServサービスインターフェイスの現在の動作ステータス

Policy Name: インターフェイスに付与されたポリシー名

注: 上記のカウンタはすべてのプラットフォームで対応しているわけではありません。対応しているカウンタのみが表示されます。

9.22 ACLコマンド

9.22.1 Showコマンド

9.22.1.1 show mac access-lists

このコマンドによりMACアドレスリスト、およびACLに定義されたすべての規則を表示します。<name>パラメータで、表示する特定のMAC ACLを識別します。

Syntax
show mac access-list <name>

<name> は表示するMAC ACLを固有に識別するACL名です。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

MAC ACL Name: MAC ACL規則名

Rule Number: ACLで定義された順列規則数の識別子

Action: 規則に関連した動作。値はPermitまたはDeny

Source MAC Address: 規則のソースMACアドレス

Source MAC Mask: 規則のソースMACマスク

Destination MAC Address: 規則の宛先MACアドレス

Destination MAC Mask: 規則の宛先MACマスク

Ethertype: 規則のEthertypE-KEYワードまたはカスタム値

VLAN ID: 規則のVLAN識別子の値または範囲

CoS Value: 規則のCOS (802.1p)の値

Secondary VLAN ID: 規則のセカンダリVLAN識別子の値または範囲

Secondary COS: 規則のセカンダリCOS (802.1p)の値

Assign Queue: 規則に一致するパケットが割り当てられているキュー識別子

Redirect Interface: 規則に一致するパケットが転送されるスロット／ポート

9.22.1.2 show mac access-lists

このコマンドによりシステム内のすべての定義済みMACアクセスリストの概要を表示します。

Syntax
show mac access-list

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Current number of all ACLs: ACLに定義されたユーザ設定規則の数

Maximum number of all ACLs: ACL規則の最大数

MAC ACL Name: MAC ACL規則名。

Rules: ACLの規則数

Direction: 列記されたインターフェイスにMAC ACLが付与される方向。値はInboundまたはOutbound

Interface/インターフェイス: MAC ACLが特定方向で付与されるインターフェイス（スロット／ポート）のリスト

9.22.1.3 show ip access-lists

このコマンドによりアクセス制御リスト（ACL）、およびACLに定義されているすべての規則を表示します。

Syntax
show ip access-lists [<1-199>]

<1-199>はACLを識別する数です。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Current number of ACLs: ACLに定義されたユーザ設定規則の数

Maximum number of ACLs: ACL規則の最大数

ACL ID: ACLの識別子

© 2010 富士通テクノロジー・ソリューションズ

Rule: ACLに定義された規則の番号識別子

Action: これは各規則と関連付けられた動作を表示します。とりうる値はPermitまたはDenyです。

Match ALL Match: すべてのパケットまたはなし

Protocol: 規則をフィルタするプロトコル

Source IP Address: 規則のソースIPアドレス

Source IP Mask: 規則のソースIPアドレスマスク

Source Ports: 規則のソースポートの範囲

Destination IP Address: 規則の宛先IPアドレス

Destination IP Mask: 規則の宛先IPマスク

Destination Ports: 規則の宛先ポートの範囲

Service Type Field Match: IP DSCP、IP Precedence、IP TOSの一致基準が規則に指定されているかを示します。

Service Type Field Value: Service Type Field Matchに指定されている値 (IP DSCP、IP Precedence、IP TOS)

9.22.1.4 show access-lists interface

このコマンドにより方向が「in」の特定インターフェイスのアクセスリスト情報を表示します。

Syntax
show access-lists interface <slot/port> in

<slot/port> はインターフェイス番号です。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

ACL Type: ACLタイプがIPまたはMACであるかを示します。

ACL ID: ACL IDを示します。

Sequence Number: インターフェイスおよび方向に関連付けられている他のアクセスリストに関連するアクセスリストの順番。順番は番号順です。

9.22.2 設定コマンド

9.22.2.1 mac access-list extended

このコマンドによりEthernetフレームのレイヤー2ヘッダーに定義された分類フィールドのある、<name>で識別されたMACアクセス制御リスト (ACL) を作成します。<name>パラメータは大文字と小文字で区別される1～31文字の英数字で、MACアドレスリストを固有に識別します。同じ名前のMAC ACLがすでに存在する場合、このコマンドでMac Access-list コンフィグモードを入力し、既存のACLを更新することができます。

Syntax
mac access-list extended <name> no mac access-list extended <name>

<name> - MACアドレスリストを固有に識別します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.22.2.2 mac access-list extended

このコマンドによりMACアクセス制御リスト (ACL) の名前を変更します。<name>パラメータは既存のMAC ACLの名前です。<newname>パラメータは大文字と小文字で区別される1～31文字の英数字で、MACアクセスリストを固有に識別します。<newname>のMAC ACL名が存在する場合、このコマンドは失敗となります

Syntax
mac access-list extended rename <name> <newname>

<name> - MACアクセスリストを固有に識別する前回の名前

<newname> - MACアクセスリストを固有に識別する新規の名前

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.22.2.3 mac access-list

このコマンドにより現在のMACアドレスリストに規則を新規作成します。各規則は、アドレスリストの設定規則リストに付与されます。「deny all」のMAC規則で、アクセスリストをつねに終了します。注記:ACL内の規則を個別に削除することはできないため、「no」のコマンドには対応していません。そのためACL全体を削除し再度指定する必要があります。

特定の分類フィールドに応じて、規則でトラフィックを拒否または許可します。少なくとも、ソースMACと宛先MACの値とマスクペアを指定する必要があり、フィールドのいずれかの値に一致することを示す「any」のキーワードで代替することができます。BPDU MACの値01-80-c2-xx-xx-xx (16進数。「xx」は不問) を示す宛先MACの値/マスクに、「bpdu」のキーワードを指定することができます。残りのコマンドパラメータはすべて任意となります。Ethertypeは、キーワード、または0x0600～0xFFFFの4桁の16進数で指定します。現在対応している<ethertypekey>の値はppletalk、arp、ibmsna、ipv4、ipv6、ipx、mplsmcast、mplsucast、netbios、novell、pppoe、rarpです。この値は、同じEthertype値に変換されます。割り当てキューのパラメータにより、特定ハードウェアキューの仕様で、この規則に一致するトラフィックを処理します。許可される<queue-id>の値は0～(n-1)で、nはハードウェアプラットフォームで使用できるユーザ設定可能キューの数です。redirectパラメータにより、この規則に一致するトラフィックを特定の<slot/port>に転送することができます。割り当てキューおよびredirectパラメータは、permit の規則のみで有効化されます。

Syntax
{deny | permit} {{<srcmac> <srcmask>} | any} {{<dstmac> <dstmask>} | any | bpdu} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {{eq <0-4095>}} [cos <0-7>] [<secondary-vlan {{eq <0-4095>}} [secondary-cos <0-7>] [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>] [<rule-id>]

初期設定

なし

コマンド・モード

Mac Access-list コンフィグ

9.22.2.4 mac access-group in

このコマンドにより特定方向のインターフェイスに、<name>で識別された特定のMACアクセス制御リスト (ACL) を付与します。<name>パラメータは既存のMAC ACLの名前である必要があります。任意のシーケンス番号で、このインターフェイスと方向に割り当てられている他のアクセスリストに関連する、アクセスリストの順番を指定します。順番は番号順です。シーケンス番号がこのインターフェイスと方向に使用されている場合、シーケンス番号を使用して、現在付与されているアクセスリストが特定のアクセスリストで置き換えられます。シーケンス番号がこのコマンドに指定されていない場合、このインターフェイスと方向で現在使用されている最大シーケンス番号より大きいシーケンス番号が使用されます。「Interface Config」モードで指定したこのコマンドは1インターフェイスのみに適用され、「Global Config」モード設定はすべてのインターフェイスに適用されます。「Interface Config」モードコマンドは、サービスキュー設定の独立ポート単位クラスに対応したプラットフォーム上のみで使用することができます。

Syntax
mac access-group <name> in [<1-4294967295>] no mac access-group <name> in

<name> - MACアドレスリストを固有に識別します。

<1-4294967295> - ACLのシーケンス番号 。

no - このコマンドにより特定方向のインターフェイスから、<name>で識別されたMAC ACLを削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ、インターフェイス・コンフィグ

9.22.2.5 access-list

このコマンドによりパラメータで識別されたアクセス制御リスト (ACL) を作成します。

Syntax
access-list {(<1-99> {deny | permit} {every | <srcip> <srcm ask>}) | ({<100-199> {deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>} any | <srcip> <srcmask> [{eq {<portvalue> | <portkey>}](any | <dstip> <dstmask>) [{eq {<portvalue> | <portkey>}] {[precedence <precedence>] | [tos <tos> <tosmask>] | [dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect} <slot/port>] [<rule-id>]}}}}})

<accesslistnumber>：ACL番号は1～199の整数です。1～99は通常のACLリスト、100～199は拡張ACLリストです。

permit or deny：ACL規則は2つのオプションで作成されます。ACL規則をフィルタするプロトコルに、icmp、igmp、ip、tcp、udpの使用を指定します。このコマンドによりsrcip and srcmask parametersで指定されたACL規則の一致基準について、ソースIPアドレスおよびソースマスクを指定します。ACL規則のソースレイヤー4ポートの一致基準は、*port value*パラメータで指定します。

<portvalue>には、domain、echo、ftp、ftpdata、http、smtp、snmp、telnet、tftp、wwwのキーワードを使用します。この値は同じポート番号に変換され、ポート範囲の開始および終了として使用されます。このコマンドにより*dstip*と*dstmask*パラメータで指定されたACL規則の一致基準について、宛先IPアドレスと宛先マスクを指定します。また、precedenceの一致状態やtos、tosmask、dscpパラメータを使用したDSCP値に応じて、ACL規則のTOSを指定します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.22.2.6 no access-list

このコマンドにより<*accesslistnumber*>パラメータで識別されたACLをシステムから削除します。

Syntax
no access-list {<1-99> | <100-199>} [<rule-id>]

<rule-id> -規則IDを追加します。

注: ACL番号は1～199の整数です。1～99は通常のACLリスト、100～199は拡張ACLリストです。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.22.2.7 ip access-group

このコマンドにより特定のアクセス制御リストをインターフェイスに付与します。

Syntax
ip access-group <1-199> in [<1-4294967295>]

<1-199> ACLの識別子。

<1-4294967295> ACLのシーケンス番号 。

初期設定

なし

コマンド・モード

グローバル・コンフィグ, インターフェイス・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.23 CoSコマンド

9.23.1 Showコマンド

9.23.1.1 show queue cos-map

このコマンドにより特定インターフェイスの内部トラフィッククラスへマッピングされている、現在のDot1p (802.1p) プライオリティを表示します。slot/portパラメータは任意で、サービスマッピングの独立ポート単位クラスに対応しているプラットフォーム上のみで有効化されます。指定した場合、インターフェイスの802.1pマッピングテーブルが表示されます。指定しない場合、最新のグローバル設定が表示されます。

Syntax
show queue cos-map <slot/port>

<slot/port> はインターフェイス番号です。

初期設定

なし

コマンド・モード

特権 Exec, ユーザ Exec /特権イネーブル、ユーザイネーブル

表示メッセージ

以下の情報は各ユーザプライオリティについて繰り返されます。

User Priority: 802.1pユーザプライオリティの値

Traffic Class/トラフィック・クラス: ユーザプライオリティがマップされるトラフィッククラスの内部キュー識別子

9.23.1.2 show queue ip-dscp-mapping

このコマンドにより内部トラフィッククラスにIP DSCPの値をマップします。<ipdscp>の値は0～63の整数のいずれか、またはキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

<trafficclass>の値は0～7ですが、使用できるトラフィッククラスの数はプラットフォームにより異なります。

Syntax
show queue ip-dscp-mapping

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

IP DSCP: IP DSCP値

Traffic Class / トラフィック・クラス: キューマッピング

9.23.1.3 show queue trust

このコマンドにより特定インターフェイスの現在の信頼モード設定を表示します。slot/portパラメータは任意で、サービスマッピングの独立ポート単位クラスに対応しているプラットフォームのみで有効化されます。指定した場合、インターフェイスのポート信頼モードが表示されます。指定しない場合、システムの各インターフェイスの信頼モードが表示されます。プラットフォームがサービスマッピングの独立ポート単位クラスに対応していない場合、すべてのインターフェイスで使用されているシステムワイドポート信頼モードが表示されます。

Syntax
show queue trust [<slot/port>]

<slot/port> はインターフェイス番号です。

初期設定

なし

コマンド･モード

特権 Exec, ユーザ Exec /特権イネーブル、ユーザイネーブル

表示メッセージ

Class of Service Trust Mode: インターフェイスの信頼モード

Non-IP Traffic Class/非IPトラフィック･クラス: 非IPトラフィックで使用されているトラフィッククラス。COSトラストモードが「trust ip-dscp」または「trust ip-precedence」に設定されている場合にのみ表示されます。

Untrusted Traffic Class/信頼されないトラフィック･クラス: 信頼性がないすべてのトラフィックに使用するトラフィッククラス。COS信頼モードが「untrusted」に設定されている場合にのみ表示されます。

9.23.1.4 show queue cos-queue

このコマンドにより特定インターフェイスのclass-of-serviceキューの設定を表示します。slot/portパラメータは任意で、サービスマッピングの独立ポート単位クラスに対応しているプラットフォームのみで有効化されます。指定した場合、インターフェイスのサービスキューのクラス設定が表示されます。指定しない場合、最新のグローバル設定が表示されます。

Syntax
show queue cos-queue [<slot/port>]

<slot/port> はインターフェイス番号です。

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Interface/インターフェイス : インターフェイスのスロット／ポートを表示します。グローバル設定を表示する場合、出力行にGlobal Configと表示されます。

Interface Shaping Rate/インターフェイス・シェイピング速度 : インターフェイスの最高送信帯域。インターフェイスのキュー単位の最高帯域の値には依存しません。値は設定可能です。

以下の値はインターフェイスの各キューについて繰り返されます。

Queue ID/キューID: インターフェイスが対応している、0～(n-1) の番号の付いたn個のキュー。nの値はプラットフォームに依存します。

Minimum Bandwidth/最小帯域: パーセンテージ表示の、キューの最低送信帯域保証。0は帯域が保証されておらずキューが最大限で動作することを示します。値は設定可能です。

Scheduler Type/スケジューラ・タイプ: 絶対優先または重み付きスキームを使用し、このキューが予定通りに送信されるかを示します。

Queue Mgmt Type /キュー管理タイプ: このキューに使用されているキュー深度管理機能。テールドロップまたは重み付きランダム早期破棄 (WRED) 。値は設定可能です。

© 2010 富士通テクノロジー・ソリューションズ

9.23.2 設定コマンド

9.23.2.1 queue cos-map

このコマンドにより802.1pプライオリティをポート単位で内部トラフィッククラスにマップします。

Syntax
queue cos-map <0-7> <0-6> no queue cos-map

<0-7> - キュープライオリティの範囲は0～7

<0-7> - マップ済みトラフィッククラスの範囲は0～7

no - キュープライオリティと、マップ済みトラフィッククラスをデフォルトマッピングに戻します。



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0～7.

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

このコマンドによりデバイスの内部トラフィッククラスに802.1pプライオリティをマップします。

Syntax
queue cos-map all <0-7> <0-6> no queue cos-map all

<0-7> - キュープライオリティの範囲は0～7

<0-7> - マップ済みトラフィッククラスの範囲は0～7

no - キュープライオリティと、マップ済みトラフィッククラスをデフォルトマッピングに戻します。



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0～7

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.23.2.2 queue ip-dscp-mapping

このコマンドによりデバイスの内部トラフィッククラスにIP precedenceをマップします。

Syntax
queue ip-dscp-mapping <ipdscp> <0-7> no queue ip-dscp-mapping

<ipdscp> - IP DSCPの値は0～63の整数のいずれか、またはIP DSCPキーワードaf11、af12、af13、af21、af22、af23、af31、af32、af33、af41、af42、af43、be、cs0、cs1、cs2、cs3、cs4、cs5、cs6、cs7、efのいずれかで指定されます。

<0-7> - マップ済みトラフィッククラスの範囲は0～7

no - IP DSCPと、マップ済みトラフィッククラスをデフォルトマッピングに戻します。



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0～7.

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

© 2010 富士通テクノロジー・ソリューションズ

9.23.2.3 queue trust

このコマンドによりインターフェイスのサービストラストモードのクラスを設定します。モードはDot1p (802.1p) 、IP Precedenceでtrustに設定することができます。

Syntax
queue trust {dot1p | ip-dscp | untrusted} no queue trust

no - このコマンドによりインターフェイスのモードをデフォルト値に戻します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

このコマンドによりすべてのインターフェイスにサービス信頼モードのクラスを設定します。モードはDot1p (802.1p) 、IP Precedenceでtrustに設定することができます。

Syntax
queue trust all {dot1p | ip-dscp | untrusted} no queue trust all

no - このコマンドによりすべてのインターフェイスのサービス信頼モードのクラスをデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.23.2.4 queue cos-queue min-bandwidth

このコマンドにより各インターフェイスキューの最低送信帯域保証を指定します。

Syntax
queue cos-queue min-bandwidth <bw-0> <bw-1> … <bw-7> no queue cos-queue min-bandwidth

<bw-0> <bw-1> … <bw-7> - 有効範囲は0～100で、5ずつインクリメントし、合計値は100以下となります。

no – このコマンドにより各キューの最低帯域値をデフォルト値に戻します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

このコマンドによりデバイスの各インターフェイスキューの最低送信帯域保証を指定します。

Syntax
queue cos-queue min-bandwidth all <bw-0> <bw-1> … <bw-7> no queue cos-queue min-bandwidth all

<bw-0> <bw-1> … <bw-7> - 有効範囲は0～100で、5ずつインクリメントし、合計値は100以下となります。

no - このコマンドによりデバイスの各キューの最低帯域値をデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.23.2.5 queue cos-queue strict

このコマンドにより各指定キューの絶対優先スケジューラモードをポート単位でアクティブ化します。

Syntax
queue cos-queue strict <queue-id-0> [<queue-id-1> … <queue-id-7>] no queue cos-queue strict <queue-id-0> [<queue-id-1> … <queue-id-7>]

no - このコマンドにより各指定キューをポート単位でデフォルトの重み付きスケジューラモードに戻します。.



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0～7

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

© 2010 富士通テクノロジー・ソリューションズ

このコマンドによりデバイスの各指定キューの絶対優先スケジューラモードをアクティブ化します。

Syntax
queue cos-queue strict all <queue-id-0> [<queue-id-1> … <queue-id-7>] no queue cos-queue strict all <queue-id-0> [<queue-id-1> … <queue-id-7>]

no - このコマンドによりデバイスの各指定キューをポート単位でデフォルトの重み付きスケジューラモードに戻します。



スタック可能接続ブレードのマップ済みトラフィッククラスの範囲は 0～7.

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.23.2.6 queue cos-queue traffic-shape

このコマンドによりインターフェイスの最高送信帯域制限値を指定します。レートシェーピングともいい、一時トラフィックバーストのオーバータイムをスムージングし、送信されたトラフィックレートがバウンドされます。

Syntax
queue cos-queue traffic-shape <bw> no queue cos-queue traffic-shape

<bw> - 有効範囲は0～100で、5ずつインクリメントします。

no - このコマンドによりシェーピングレートの値をデフォルト値に戻します。

初期設定

なし

コマンド・モード

インターフェイス・コンフィグ.

このコマンドによりすべてのインターフェイスの最高送信帯域制限値を指定します。レートシェーピングともいい、一時トラフィックバーストのオーバータイムをスムージングし、送信されたトラフィックレートがバウンドされます。

Syntax
queue cos-queue traffic-shape all <bw> no queue cos-queue traffic-shape all

<bw> - 有効範囲は0～100で、5ずつインクリメントします。.

no - このコマンドによりすべてのインターフェイスのシェーピングレートの値をデフォルト値に戻します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ.

9.24 スタッキングコマンド

9.24.1 Showコマンド

9.24.1.1 show switch

このコマンドによりスタックシステム内のスタックメンバーの情報を表示します。スタッキング機能のあるEthernet接続ブレードのみで使用することができます。

Syntax
show switch [<unit>]

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

SW#: ユニットのID。スタックのユニット最大許可数は8

ID: IBPのインターフェイスを識別するために使用する、ユニットの識別子

Role: ユニットがスタックマスターであるかスタックメンバーであるかを示します。

- Mgmt Switch
- Stack Member
- Unassigned

Mac Address: IBPのMACアドレス

Priority/プライオリティ : IBPのプライオリティ。範囲は0～15、値はunassignedまたはdisabled

Current Status/現在の状態 : IBPのステータス

- Ready
- Not Ready
- Unsupported
- Code Mismatch
- Config Mismatch
- Not Present
- Code Updating

Version /バージョン: この欄はユニットに検出されたコードのバージョンを示す。

9.24.1.2 show switch stack port

このコマンドによりスタックシステム内のスタックメンバーのスタックポート情報を表示します。スタッキング機能のあるEthernet接続ブレードのみで使用することができます。

Syntax
show switch stack-port

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Unit/ユニット: ユニットを表示する。.

Interface/インターフェイス: 所与のユニットにあるスタック可能インターフェイスを表示する。

Configured Stack Mode/構成スタック・モード: 所与のインターフェイスに構成されたモードを表示する。Currently, only N/A is displayed.

Running Stack Mode/実行スタック・モード: スタック可能インターフェイスの実行時モードを表示する。

Link Status/リンク・ステータス ： スタッキングポートのリンクステータス (UP／DOWN)

Link Speed (Gb/s)/リンク速度 ： スタック・ポートの最高速度を表示する。

9.24.1.3 show stack port counter statistic

このコマンドによりスタッキングポートの統計データを表示します。スタッキング機能のあるEthernet接続ブレードのみで使用することができます。

Syntax
show switch stack-port counters [detailed]

初期設定

なし

コマンド・モード

特権 EXEC

表示メッセージ

Unit/ユニット - ユニットを表示する。.

Interface/インターフェイス - 所与のユニットにあるスタック可能インターフェイスを表示する。

送受信統計

Data Rate (Mb/s)/データ速度 - スタック・ポート上の速度概数を表示する。

Error Rate (Errors/s): スタック・ポート上のエラー頻度概数を表示する。

Total Errors/合計エラー数 - 起動以降のエラー合計値を表示する。 カウンターはラップできる。

© 2010 富士通テクノロジー・ソリューションズ

9.24.2 設定コマンド

9.24.2.1 スイッチのプライオリティを設定する

このコマンドによりIBPのプライオリティを設定します。IBPのプライオリティを上げると、スタックシステムでスタックマスターになる確率が高くなります。

Syntax
switch <unit> priority <0-15> no switch <unit> priority

<unit> - IBPのユニット番号。範囲は1～8

<0-15> - プライオリティの値。範囲は0～15

no - このコマンドによりプライオリティの値をunassignedに戻します。

初期設定

Unassigned

コマンド・モード

グローバル・コンフィグ

© 2010 富士通テクノロジー・ソリューションズ

9.24.2.2 switch provision

このコマンドにより新規IBPを設定します。物理IBPがスタックシステムに接続する前にIBPを再度設定することができます。

Syntax
switch <unit> provision no switch <unit> provision

<unit> - IBPのユニット番号。範囲は1～8

no - このコマンドによりIBPの設定を削除します。

初期設定

なし

コマンド・モード

グローバル・コンフィグ

9.24.2.3 IPBから別のIBPへ管理制御を移動する

このコマンドにより管理IBPを別のIBPへ移動します。

Syntax
switch movemanagement <fromunit> <tounit>

<fromunit> - IBPのユニット番号。範囲は1～8

<tounit> - IBPのユニット番号。範囲は1～8

初期設定

なし

コマンド･モード

グローバル･コンフィグ

© 2010 富士通テクノロジー･ソリューションズ

10　SNMPを使用する

SNMP（シンプルネットワーク管理プロトコル）は、ネットワーク上のデバイスやその他のエレメントを管理するため設計された通信プロトコルです。SNMPは、IBP、ルータ、ホストコンピュータの共通管理を行います。SNMPは通常、ネットワーク環境でこうしたデバイスが正しく動作するための設定に使用します。またデバイスの監視も行い、動作の評価や、発生するおそれのある問題を検出します。

SNMPを使用してネットワーク管理ステーションからIBPにアクセスするには、以下の手順で行います。

1. ホストコンピュータ上に SNMP 管理アプリケーションをインストールします。
2. 管理ステーションを検証し、ステーションと IBP を同じ IP ドメインに設定します。
3. SNMP からのネットワーク管理アクセスを行うため、コミュニティー名とアクセス権を設定します。
4. IBP からトラップメッセージを受信するには、トラップマネージャの IP アドレス、関連コミュニティー名、IBP から作成されるトラップタイプを指定する必要があります。
5. SNMP 管理ステーションは、管理情報ベース（MIB）で指定されたデバイス変数の設定または読み取りを行い、ネットワークデバイスを設定、監視することができます。IBP が対応しているキーMIB グループは、補遺に列記されています。

ネットワーク管理システムからデバイスステータスを監視する、またはIBP上のシステムパラメータを修正するには、SNMP管理アプリケーションから正しいMIB変数にアクセスする必要があります。

© 2010 富士通テクノロジー・ソリューションズ

10.1　対応MIB

標準MIBは以下のとおりです。

仕様	パブリックMIB名	MIBファイル
IEEE 802.1x	IEEE8021-PAE-MIB	dot1x.my
IEEE 802.3ad	LAG-MIB	dot3ad.my
RFC 1213	RFC1213-MIB	mib-2.my
RFC 2011	IP-MIB	RFC2011 ip-icmp.my
RFC 1493	BRIDGE-MIB	bridge.my
RFC 1643	ETHERLIKE-MIB	etherlike.my
RFC 1907	SNMPv2-MIB	v2-mib.my
RFC 2233	IF-MIB	if.my
RFC 2571	SNMP-FRAMEWORK-MIB	v3-arch.my
RFC 2572	SNMP-MPD-MIB	v3-mpd.my
RFC 2573	SNMP-TARGET-MIB	v3-tgt.my
RFC 2574	SNMP-USER-BASED-SM-MIB	v3-usm.my
RFC 2575	SNMP-VIEW-BASED-ACM-MIB	v3-acm.my
RFC 2576	SNMP-COMMUNITY-MIB	coex.my
RFC 2618	RADIUS-AUTH-CLIENT-MIB	radius_auth_client.my
RFC 2620	RADIUS-ACC-CLIENT-MIB	radius_acc_client.my
RFC 2674	P-BRIDGE-MIB Q-BRIDGE-MIB	pbridge.my vlan.my
RFC 2737	ENTITY-MIB	entity.my
RFC 2819	RMON-MIB	rmon.my
RFC 3289	DIFFSERV-MIB DIFFSERV-DSCP-TC	diffserv.my, diffserv_dscp_tc.my
RFC 2932	IANA-RTPROTO-MIB	rtproto.my
RFC 2668	MAU-MIB	rfc2668.my
RFC 2213	INTEGRATED-SERVICES-MIB	intserv.my
RFC 3291	INET-ADDRESS-MIB	inetaddress.my
RFC 1573	IANAifType-MIB	iftype.my
RFC 2677	IANA-ADDRESS-FAMILY-NUMBERS-MIB	ianaaddr.my

© 2010　富士通テクノロジー・ソリューションズ

プライベートエンタープライズMIBは以下のとおりです。

プライベートMIB名	MIBファイル
FSC-SWITCH-MIB	fscref.my
OUTBOUNDTELNET-PRIVATE-MIB	telnet.my
MGMT-SECURITY-MIB	mgmt_security.my
DENIALOFSERVICE-PRIVATE-MIB	dos.my
COS-MIB	qos_cos.my
QOS-MIB	qos.my
QOS-ACL-MIB	qos_acl.my
QOS-DIFFSERV-EXTENSIONS-MIB	qos_diffserv_extensions.my
QOS-DIFFSERV-PRIVATE-MIB	qos_diffserv_private.my
RADIUS-CLIENT-PRIVATE-MIB	radius.my
RADIUS-ACC-CLIENT-MIB	radius_acc_client.my
RADIUS-AUTH-CLIENT-MIB	radius_auth_client.my
TACACS-CLIENT-MIB	tacacsclient.my
INVENTORY-MIB	inventory.my
LOGGING-MIB	logging.my
SNTP-CLIENT-MIB	sntp.my
SWITCHING-MIB	switching.my
PORTSECURITY-PRIVATE-MIB	portsecurity.my
SWITCHING-EXTENSION-MIB	switching_extension.my

© 2010 富士通テクノロジー・ソリューションズ

10.2 MIBオブジェクトにアクセスする

MIBオブジェクトは、SNMPアプリケーションが制御、管理できるIBPの機能を表示します。例えばRFC-2233 IF-MIBグループを使用し、MIBグループの異なる変数を読み取りまたは書き込み、ポート設定を取得、設定することができます。このグループが対応している変数は以下のとおりです。

RFC 2233 IF-MIB		
interfaces		
ifNumber	*Yes	*RO
ifMIBObjects		
ifTableLastChange	*No	RO
ifStackLastChange	No	RO
ifTable	Index:	ifIndex
ifDescr	Yes	RO
ifType	Yes	RO
ifMtu	Yes	RO
ifSpeed	Yes	RO
ifPhysAddress	Yes	RO
ifAdminStatus	Yes	*RW
ifOperStatus	Yes	RO
ifLastChange	Yes	RO
ifInOctets	Yes	RO
ifInUcastPkts	Yes	RO
ifInNUcastPkts	Yes	RO
ifInDiscards	Yes	RO
ifInErrors	Yes	RO
ifInUnknownProtos	No	RO
ifOutOctets	Yes	RO
ifOutUcastPkts	Yes	RO
ifOutNUcastPkts	Yes	RO
ifOutDiscards	No	RO
ifOutErrors	Yes	RO
ifOutQLen	No	RO
ifSpecific	No	RO
ifXTable	Index:	ifIndex
ifName	Yes	RO
ifInMulticastPkts	Yes	RO
ifInBroadcastPkts	Yes	RO
ifOutMulticastPkts	Yes	RO
ifOutBroadcastPkts	Yes	RO
ifHCInOctets	Yes	RO

© 2010 富士通テクノロジー・ソリューションズ

ifHCInUcastPkts	Yes	RO
ifHCInMulticastPkts	Yes	RO
ifHCInBroadcastPkts	Yes	RO
ifHCOutOctets	Yes	RO
ifHCOutUcastPkts	Yes	RO
ifHCOutMulticastPkts	Yes	RO
ifHCOutBroadcastPkts	Yes	RO
ifLinkUpDownTrapEnable	Yes	RW
ifHighSpeed	Yes	RO
ifPromiscuousMode	Yes	RO
ifConnectorPresent	Yes	RO
ifAlias	No	RW
ifCounterDiscontinuityTime	Yes	RO
ifStackTable	Indicies:	ifStackHigherLayer, ifStackLowerLayer
ifStackStatus	No	*RC
ifRcvAddressTable	Indicies:	ifIndex, ifRcvAddressAddress
ifRcvAddressStatus	No	RC
ifRcvAddressType	No	RC
ifTestTable	Index:	ifIndex
ifTestId	No	RW
ifTestStatus	No	RW
ifTestType	No	RW
ifTestResult	No	RO
ifTestCode	No	RO
ifTestOwner	No	RW

*注記:

Yes – 対応

No – 非対応

RW - 読み取り・書き込み可

RO - 読み取り専用

RC – 読み取り・作成可

10.3 対応トラップ

対応しているSNMPトラップは以下のとおりです。

RFC No	Title
RFC 1215	coldStart warmStart linkDown linkUp authenticationFailure
RFC 2819	risingAlarm fallingAlarm

© 2010 富士通テクノロジー・ソリューションズ

PRIMERGY
スイッチブレード (1Gbps 36/8+2) (PG-SW111)
スイッチブレード (1Gbps 36/12) (PG-SW112)
IBPユーザーズガイド

CA92276-8604-02

発行日　2010年12月
発行責任　富士通株式会社

●本書の内容は、改善のため事前連絡なしに変更することがあります。
●本書に記載されたデータの使用に起因する、第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。
●無断転載を禁じます。